IMPLEMENTATION OF THE COMPUTER SECURITY ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY HOUSE OF REPRESENTATIVES

ONE HUNDREDTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 1988

[No. 146]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE

90-130 WASHINGTON : 1989

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

H701-38

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

ROBERT A. ROE, New Jersey, *Chairman*

GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY L. BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
JAMES A. TRAFICANT, JR., Ohio
JIM CHAPMAN, Texas
LEE H. HAMILTON, Indiana
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
C. THOMAS McMILLEN, Maryland
DAVID E. PRICE, North Carolina
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
DAVID E. SKAGGS, Colorado
PAUL E. KANJORSKI, Pennsylvania
GEORGE J. HOCHBRUECKNER, New York

MANUEL LUJAN, JR., New Mexico*
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, JR., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID MORRISON, Washington
RON PACKARD, California
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, JR., Virginia
LAMAR SMITH, Texas
ERNEST L. KONNYU, California
JACK BUECHNER, Missouri
JOEL HEFLEY, Colorado
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
CAROLYN C. GREENFELD, *Chief Clerk*
R. THOMAS WEIMER, *Republican Staff Director*

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

DAVE McCURDY, Oklahoma, *Chairman*

DAN GLICKMAN, Kansas
BILL NELSON, Florida
C. THOMAS McMILLEN, Maryland
JIMMY HAYES, Louisiana

TOM LEWIS, Florida
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, JR., Wisconsin

---

*Ranking Republican Member.

CONTENTS

WITNESSES

	Page
September 22, 1988:	
Jay Plager, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget	7
RADM W.O. Studeman, U.S. Navy, Director; Dr. James J. Hearn, Deputy Director for Information Security, National Security Agency; accompanied by Patrick R. Gallagher, Jr., Director, National Computer Security Center	22
Raymond G. Kammer, deputy director, National Institute of Standards and Technology, accompanied by James Burrows, director, National Computer and Telecommunications Laboratory	51
John J. Lafferty, Deputy Associate Director for Training and Investigations, Office of Personnel Management	70
Francis A. McDonough, Deputy Commissioner, Federal Information Resources Management, General Services Administration	87
Howard G. Rhile, Jr., Associate Director, Information Management and Technology Division, General Accounting Office	94

IMPLEMENTATION OF THE COMPUTER SECURITY ACT

THURSDAY, SEPTEMBER 22, 1988

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 2325, Rayburn House Office Building, Hon. Dave McCurdy (chairman of the subcommittee) presiding.

Staff present: Anthony C. Taylor, staff director; Dr. James C. Greene, republican science consultant; Dr. Harold J. Podell, technical consultant.

Mr. MCCURDY. The subcommittee will now come to order. I thank the gentleman from Wisconsin.

On January 8, 1988, the President signed landmark legislation that will have a wide ranging effect on Federal Government operations. This legislation is the Computer Security Act of 1987, Public Law 100-235.

The Computer Security Act represents the culmination of several years of hard work by members of this Subcommittee, our colleagues from the Subcommittee on Science, Research, and Technology, and other members of the Science, Space, and Technology Committee, members of the Government Operations Committee, and we certainly can't forget the distinguished Chairman of that Committee, and many in the Executive Branch.

The purpose of the Act is to improve the security and privacy of sensitive information contained in government computers. The Subcommittee found during several years of investigation, that all kinds of government data, such as IRS records, Food Stamp payments and air traffic control data, are vulnerable to unauthorized access and manipulation.

Furthermore, we found a distressing lack of leadership within the government in dealing with this serious problem. The result was the Computer Security Act of 1987, which lays out for the first time, a plan for improving computer security government wide. The purpose of this hearing is to review the progress being made by the federal agencies in implementing the Act.

We will also assess the efforts of all federal agencies in implementing the Act, including a review of their progress in identifying sensitive information systems, a milestone that came due last July.

I view this hearing as significant because new programs such as this enter a critical period immediately after their enactment.

Either everyone gets on board and the program becomes institutionalized, or the Act dies of neglect. We are in this critical period right now, so we want to assure ourselves that each of the Act's major milestones are being or will be met. We are fortunate to have representatives from each of the key agencies here today to give us the status on the progress. We look forward to their testimony and to a discussion of any problems that they have encountered.

Finally, I'd like to note for the record, my perception that all the key players appear to be working hard to make the Act successful. I'd especially like to commend OMB for the leadership it has demonstrated. In the past, I characterized that agency as a reluctant dragon and a few other things at different times. Anyway, since the Subcommittee began working on early drafts of the Computer Security Act with Frank Reeder and his staff, I've seen a dramatic change.

I'd like to acknowledge publicly his leadership, commitment and hard work. Also, having spent five years on the Government Select Committee on Intelligence, I understand that there may be some questions that may open the door to classified information, and we will be mindful of that. If we do broach those subjects, then feel free to raise a hand, or something and tell us that we probably ought to discuss that in a closed session or follow up in some way. I don't expect that to hamper the frankness or candidness of the witnesses today.

[The prepared statements Mr. McCurdy and Mr. Lewis follow:]

THE HONORABLE DAVE MCCURDY, CHAIRMAN
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

SEPTEMBER 22, 1988

THE COMPUTER SECURITY ACT OF 1987
(PUBLIC LAW 100-235)

ON JANUARY 8, 1988, THE PRESIDENT SIGNED LANDMARK LEGISLATION THAT WILL HAVE A WIDE RANGING EFFECT ON FEDERAL GOVERNMENT OPERATIONS. THIS LEGISLATION IS THE COMPUTER SECURITY ACT OF 1987 -- PUBLIC LAW 100-235. THE COMPUTER SECURITY ACT REPRESENTS THE CULMINATION OF SEVERAL YEARS OF HARD WORK BY MEMBERS OF THIS SUBCOMMITTEE; OUR COLLEAGUES FROM THE SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY; OTHER MEMBERS OF THE SCIENCE, SPACE, AND TECHNOLOGY COMMITTEE; MEMBERS OF THE GOVERNMENT OPERATIONS COMMITTEE; AND MANY IN THE EXECUTIVE BRANCH.

THE PURPOSE OF THE ACT IS TO IMPROVE THE SECURITY AND PRIVACY OF SENSITIVE INFORMATION CONTAINED IN GOVERNMENT COMPUTERS. THE SUBCOMMITTEE FOUND, DURING SEVERAL YEARS OF INVESTIGATION THAT ALL KINDS OF GOVERNMENT DATA -- SUCH AS IRS RECORDS, FOOD STAMP PAYMENTS AND AIR TRAFFIC CONTROL DATA -- ARE VULNERABLE TO UNAUTHORIZED ACCESS AND MANIPULATION. FURTHERMORE, WE FOUND A DISTRESSING LACK OF LEADERSHIP WITHIN THE GOVERNMENT IN DEALING WITH THIS SERIOUS PROBLEM. THE RESULT WAS THE COMPUTER SECURITY ACT OF 1987, WHICH LAYS OUT, FOR THE FIRST TIME, A PLAN FOR IMPROVING COMPUTER SECURITY GOVERNMENT WIDE.

PAGE TWO

THE PURPOSE OF THIS HEARING IS TO REVIEW THE PROGRESS BEING MADE BY THE FEDERAL AGENCIES IN IMPLEMENTING THE ACT. OUR FOCUS WILL BE ON THE EFFORTS OF THE AGENCIES NAMED IN THE ACT. BUT WE WILL ALSO ASSESS THE EFFORTS OF ALL FEDERAL AGENCIES IN IMPLEMENTING THE ACT, INCLUDING A REVIEW OF THEIR PROGRESS IN IDENTIFYING SENSITIVE INFORMATION SYSTEMS, A MILESTONE THAT CAME DUE LAST JULY.

I VIEW THIS HEARING AS SIGNIFICANT BECAUSE NEW PROGRAMS SUCH AS THIS ONE ENTER A CRITICAL PERIOD IMMEDIATELY AFTER THEIR ENACTMENT. EITHER EVERYONE GETS ON BOARD AND THE PROGRAM BECOMES INSTITUTIONALIZED OR THE ACT DIES OF NEGLECT. WE ARE IN THIS CRITICAL PERIOD RIGHT NOW. SO WE WANT TO ASSURE OURSELVES THAT EACH OF THE ACT'S MAJOR MILESTONES ARE BEING OR WILL BE MET.

WE ARE FORTUNATE TO HAVE REPRESENTATIVES FROM EACH OF THE KEY AGENCIES HERE TODAY TO GIVE US A STATUS ON THEIR PROGRESS. WE LOOK FORWARD TO THEIR TESTIMONY AND TO A DISCUSSION OF ANY PROBLEMS THEY HAVE ENCOUNTERED.

FINALLY, I WOULD LIKE TO NOTE FOR THE RECORD, MY PERCEPTION THAT ALL THE KEY PLAYERS APPEAR TO BE WORKING HARD TO MAKE THE ACT SUCCESSFUL. I'D ESPECIALLY LIKE TO COMMEND OMB FOR THE LEADERSHIP IT HAS DEMONSTRATED. IN THE PAST I CHARACTERIZED THAT AGENCY AS A RELUCTANT DRAGON. BUT SINCE THE SUBCOMMITTEE BEGAN WORKING ON EARLY DRAFTS OF THE COMPUTER SECURITY ACT WITH FRANK REEDER AND HIS STAFF, I HAVE SEEN A DRAMATIC CHANGE. SO I WOULD LIKE TO ACKNOWLEDGE PUBLICLY FRANK'S LEADERSHIP, COMMITMENT AND HARD WORK.

HON. TOM LEWIS (R-FL)
OPENING STATEMENT
HEARING ON COMPUTER SECURITY P.L. 100-235
SEPTEMBER 22, 1988

THANK YOU, MR. CHAIRMAN.

THE IMPORTANCE OF MAINTAINING EFFECTIVE COMPUTER SECURITY INCREASES DAILY. THE FEATURE STORY IN THIS WEEK'S TIME MAGAZINE IS ON THE VIRUS EPIDEMIC IN THE COMPUTER WORLD.

AS YOU KNOW MR. CHAIRMAN, A COMPUTER VIRUS IS AN ILLEGALLY PLACED SMALL PROGRAM IN THE SOFTWARE PACKAGE THAT CAN COMMAND THE DATA BASE TO SELF DESTRUCT. THE TIME ARTICLE POINTS OUT THAT IN THE PAST NINE MONTHS, 250,000 COMPUTERS HAVE BEEN HIT WITH A VIRUS. ONE VIRUS, CALLED SCORES, HAS BEEN FOUND IN APPLE MACINTOSH COMPUTERS AT NASA, IRS AND THE U.S. HOUSE OF REPRESENTATIVES.

THE PROBLEM IS SERIOUS. THIS PAST TUESDAY A FORMER COMPANY PROGRAMMER WAS CONVICTED OF DESTROYING 168,000 RECORDS OF SALES COMMISSIONS USING A VIRUS. UNFORTUNATELY, THERE IS NO FOOL PROOF ANTIVIRAL PROGRAM. HOWEVER, PUBLIC LAW 100-235 IS A STEP IN THE DIRECTION OF PROTECTING FEDERAL COMPUTERS.

THE COMPUTER SECURITY ACT HAD A CONTROVERSIAL PAST ESPECIALLY IN DEFINING THE DUTIES OF NSA AND NBS. BOTH AGENCIES APPEAR TO BE WORKING OUT THEIR DIFFERENCES SUCCESSFULLY. NOW I HOPE WE CAN TURN OUR ATTENTION TO IMPROVING FEDERAL COMPUTER SECURITY.

THANK YOU, MR. CHAIRMAN.

Mr. McCURDY. Our first witness is Jay Plager, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget. Sir, your full testimony is admitted in its entirety in the record, and feel free to summarize or go any way you want.

STATEMENT OF JAY PLAGER, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. PLAGER. Thank you, Mr. Chairman. I will be sure to convey your remarks to Director Miller. He doesn't often get messages like that, and I know he will be delighted to hear yours.

Mr. McCURDY. I didn't send him one on the Critical Materials Council, but that was a little different sub-agency, but on this one he's been all right.

Mr. PLAGER. Mr. Chairman, members of the Subcommittee, I appreciate the opportunity to describe the Office of Management and Budget's participation in the Administration's program to implement the Computer Security Act of 1987, Public Law 100-235. I commend the Committee for the timeliness of this particular hearing.

I saw the most recent issue of Time.

Mr. McCURDY. I did refer in the opening that I was going into questions. You're right.

Mr. PLAGER. Computer viruses—that is only one aspect of what we'll be talking about today, but I couldn't help think how timely this hearing was.

OMB has long had an interest in assuring adequate security of federal automated information systems, because appropriate security of our automated information systems is essential for the conduct of government. Today, government depends on the use of advanced computers and telecommunications.

It's hard to imagine a system of Social Security such as ours, distributing more than $200 billion each year to its 39 million beneficiaries without automation; or collecting a trillion dollars in tax revenues or processing the 191 million tax returns each year. Nor could we assure the safety of 150 million aircraft operations in our skies each year. Even the system by which we make the laws of our land, now are dependent upon automation to type set and print bills, and tally votes.

These activities would be threatened without adequate security of the computer systems that support them. Just this brief listing clearly demonstrates that computer security goes beyond locking up computer rooms or encrypting data lines to protect confidential information. It also involves making sure that information is and remains accurate and that our systems work and remain reliable. For example, for many of the systems that concern us, like the hurricane forecasting system, it is accuracy and reliability that constitute the primary protection need, rather than confidentiality.

As I noted, OMB's interest in computer security is not new. Some of our past initiatives dating back more than ten years, are enumerated in my written statement. More recently, OMB worked closely with this Subcommittee, as well as the Subcommittee on

Science, Research and Technology of the Science, Space, and Technology Committee, and the Government Operations Committee, to develop and secure enactment of the Computer Security Act of 1987.

We strongly supported its enactment and have been working since then on its implementation. The Act was signed and went into effect just this year. Admittedly, it is still too early to fully assess the effectiveness. Agencies are just starting to develop computer security plans and conduct training programs. Over the coming months and years, we will begin to see the real effect of the Act on security.

At the same time, passage of the Act in and of itself, has heightened the awareness of security risks in information technology. For example, more than 600 people attended a recent workshop on computer security conducted at the National Institute of Standards and Technology. Let me enumerate a few of the things we have already done to assure achievement of the purposes of the Act.

In his budget for 1989, the President proposed doubling the budget for NIST computer security activities.

In July of this year, working with NIST and NSA staff, OMB issued guidance to agencies on computer security planning. On July 8th, we along with NIST, NSA and OPM, cosponsored the workshop I mentioned for federal employees on implementation of the training and planning portions of the Act. NIST and NSA are setting up a joint working group to review agency security plans.

In my prepared statement which I have submitted for the record, I describe in more detail, the progress that has been made in the area of computer security planning, in security awareness and training, and the development of guidelines and standards, and in coordination of agency activities, particulary NIST and NSA.

These are specific areas that I am confident the other witnesses will be addressing this morning in their remarks, and about which you may have particular questions. Rather than prolong this part of my opening statement, let me conclude by saying that I want to assure the Subcommittee of OMB's continuing commitment to making the government's computer and telecommunications resources secure in all the meanings of that term.

As I have outlined, we are actively moving to implement the Computer Security Act of 1987. We believe that the Act gives us a framework and provides the momentum for the government to address the security of federal computer systems, and we believe that the agencies have made a good start. We look forward to continuing to work closely with the Subcommittee on this important effort. I will be pleased to answer any questions that the Subcommittee may have.

[The prepared statement of Mr. Plager follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF JAY PLAGER
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
OF THE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES
ON IMPLEMENTATION OF THE COMPUTER SECURITY ACT OF 1987

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to describe the Office of Management and Budget's (OMB's) efforts to implement the Computer Security Act of 1987 (P.L. 100-235). OMB has long had an interest in assuring adequate security of Federal automated information systems because appropriate security of our automated information systems is essential to the conduct of government.

Next year the Federal government will invest more than $17 billion in building and maintaining Federal information technology systems -- systems which are critical to every major activity of our government. More importantly, while the investment in technology is large, its impact on the business of government is even more immense. It is inconceivable, for example, that a system of social security such as ours could distribute more than $200 billion each year to its 39 million beneficiaries without automation. Nor could tax revenue be collected or the 191 million tax returns be processed each year. Nor could we assure the safety of 150 million aircraft operations in our skies each year. Nor could our military be supplied without automated logistics support. Nor could we effectively operate virtually any other government program. Even the system by which we make the laws of our land is now dependent upon automation to type set and print bills and tally votes.

These activities could not be accomplished without adequate security of the computer systems that support them. Consider the impact on our ability to provide social security benefits and the risk to our assets if the computer system supporting our social security program processed inaccurate information. Or the public reaction if the computer systems that support our tax collection system improperly processed returns or did not assure the confidentiality of the information in those returns. Or the risk to safety if the computers supporting our air traffic control system or weather forecasting were rendered ineffective. Or our ability to defend the nation if the computers used to manage our logistics contained inaccurate or out of date information or were not available.

A successful computer security program in the Federal government will assure that these remain only theoretical questions.

Definition of Security

As you can see by the breadth of our concerns, computer security goes beyond locking up computer rooms or encrypting data lines. To us, security means assuring that computer systems do exactly what they are supposed to do, and nothing more. That implies assuring the confidentiality, the integrity, and the availability of the system. Confidentiality means protecting information in the system from unauthorized disclosure. Integrity means protecting information from unauthorized or inadvertent modification. Availability means that information in the system is available on a timely basis. It is important to note that in many of the systems that concern us, like the hurricane forecasting system, confidentiality is not the primary protection need. In fact, we want that information to get out.

The Computer Security Act of 1987 encompasses these three areas of concern within its definition of information requiring protection:

> "the term 'sensitive information' means any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy;" [Sec 3 of P.L. 100-235].

Historical Perspective

Recognizing that computer security was far more than a secrecy or confidentiality issue, OMB some 10 year's ago issued Transmittal Memorandum No. 1 to Circular No. A-71 entitled, "Security of Federal Automated Information Systems." At that time OMB was trying to stimulate Federal agency attention to this issue. That Memorandum directed Executive agencies to establish computer security programs and prescribed a minimum set of security requirements to be included in those agency programs. Subsequently, in 1983, OMB Circular No. A-123, "Internal Controls," required agencies to establish programs to review the adequacy of controls in their automated information systems. In 1985 OMB updated the original Circular No. A-71 by issuing OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems." While these efforts contributed to the security of Federal systems, more needed to be done.

Accordingly, last year OMB worked with this Subcommittee as well as the Subcommittee on Science, Research and Technology of the Science, Space and Technology Committee, and the Government Operations Committee to develop and secure enactment of the Computer Security Act of 1987. We strongly supported its enactment and have been working since then on its implementation.

I might note that passage of the Act in and of itself has heightened the awareness of security risks in information technology. More than 600 people attended a recent workshop on computer security conducted at the National Institute of Standards and Technology (NIST). In addition, since enactment of P.L. 100-235, NIST and OMB staff have been receiving far more inquiries concerning security of agency systems. That increase in awareness gives us a good start toward enhancing the security of Federal systems.

In the period since passage of the Act, new evidence of our security vulnerability has also appeared:

- A GAO report published in May of 1988, indicated that as recently as last year agencies continued to build systems without assurance that adequate security was being built into those systems.

- A report to the President's Council on Integrity and Efficiency this summer pointed out the lack of effective security policy in a number of Federal agencies.

Such findings are important reminders that the "bottom line" of the Computer Security Act is to enhance the security of our computer systems. While the processes we put in place to implement the Act are important, they are only valuable to the extent that they contribute to actually securing our systems.

Implementation Activities

Since the President signed P.L. 100-235, on January 8, 1988, OMB has been working with the other key agencies to assure its effective implementation:

- In his budget for 1989, the President proposed doubling the budget for NIST computer security activities.

- OMB staff have been meeting regularly with senior staff of NIST, the National Security Agency (NSA), and the Office of Personnel Management (OPM) to assure that their activities under the Act are consistent and mutually supportive. I am advised that a strong spirit of cooperation and commitment to the objectives of the Act has marked this effort.

- In May, as part of our annual call (OMB Bulletin 88-11) for agency information systems and technology plans required by the Paperwork Reduction Act of 1980, we pointed out the specific responsibilities that the Computer Security Act placed on agencies and asked them to report what they were doing to fulfill those responsibilities as part of their plans.

- In July, working with NIST and NSA staff, we issued guidance to agencies on computer security planning in OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information."

- On July 8 we, along with NIST, NSA and OPM, cosponsored a workshop for Federal employees on implementation of the training and planning portions of the Act.

- Earlier this month, we circulated answers to a list of common questions that agencies have been asking concerning implementation of the Act.

Computer Security Planning

As you know, the planning process prescribed in the Computer Security Act called for agencies to have identified those systems that contain sensitive information by July 8, 1988. By January 8, 1989, agencies are to send a copy of a plan for the security of each such system to NIST and NSA for advice and comment. Those plans are subject to OMB disapproval. A summary of such plans is also to be included in the agency's five-year plan required by the Paperwork Reduction Act.

We have been working closely with NIST and NSA to coordinate this planning process. As I mentioned earlier, we worked together to develop OMB Bulletin No. 88-16 to assist agencies in preparing computer security plans. NIST and NSA are planning a joint review of each plan, with a goal of responding to each plan submitted within 90 days.

The submission and review process is designed to produce better security plans and thus ultimately better security of computer systems. It is not a "gotcha game." For this reason, we intend to use the OMB disapproval authority only when and if agencies are non-responsive to the requirements of the Act. We also see the first year as a diagnostic phase, in which we can learn more about where additional guidance may be required.

Security is a fundamental element in building a system. The question should never be whether we build a system with or without security. We must always build systems that have adequate security. Either we build them right, or we should not build them at all. Thus we should build in access controls, or

redundancy, or administrative procedures at the front, not as later add-ons. That implies that we should not consider funding for security as a separate question from funding of the system itself. It also means we should not plan for or fund the building of systems that do not have adequate security. To do so would be tantamount to building houses without stairs, doors and locks, roofs or smoke detectors.

The Computer Security Act recognizes the need to integrate computer security into systems planning and mandates that summaries of computer security plans be included in agency's annual five-year plan required by the Paperwork Reduction Act. This gives us clear direction to integrate the computer security planning process into our general planning and budgeting processes for information technology. During the next year, we will be developing guidance for the agencies to tie these two processes together and thus assure that security planning decisions are integral to basic decisions about information technology systems.

Security Awareness and Training

The security planning process established under section 6 of the Act is not an end in itself. Rather, it is one important element in improving the security of Federal computer systems quickly. The Act also recognizes that security awareness is as important as security planning.

A key thrust of the Act is that security awareness and training applies not just to computer and computer security professionals, but also to users of systems. Such awareness is essential to improving the security of the systems. After all, it is the users of computer systems, those in the business of running government programs, be they delivering social security benefits, collecting revenues, assuring the safety of our skies or delivering material to military units, who must live with the security risk of the systems that support their programs. They must understand how much risk that entails and how they can effectively reduce that risk to an acceptable level.

That challenge is enormous. Thanks to the dramatic growth in the availability and power of computer technology, computer security is now everyone's concern. Every user of a personal computer or terminal needs to understand the level of exposure he or she has and the steps available to mitigate that risk. That does not necessarily mean deploying expensive security technology or giving everyone a three day course in technical security. It may be as simple as making sure that users know that information requiring confidentiality protection is not to be processed on unsecure devices or making sure that copies of files are periodically backed up to avoid disruptions of service.

As I mentioned earlier, passage of the Computer Security Act, in and of itself has begun the process of broadening computer security awareness within the Federal community. Issuance of the Office of Personnel Management regulation governing security awareness training and security practices for Federal employees in July should build on that momentum. Development of NIST's security training guidelines should further stimulate this activity as agencies proceed to implement their training programs.

Guidelines and Standards

Creating awareness of the security threat and conducting training are not enough. Once awareness is created, viable tools must be available for system managers to tighten the security of their systems. For the interim, we must make the best use of available tools. For the longer term, however, better tools need to be developed. To this end, NIST, drawing upon NSA technical guidelines, is tasked under the Act to develop computer security standards and guidelines. Such standards and guidelines can themselves be tools for security, such as a risk analysis guideline, or can lead to standardized commercial security products, such as products that conform to the data encryption standard in Federal Information Processing Standard No. 46.

Here NIST and NSA will also use the processes established by the Act to help. One important benefit to be derived from review of agency security plans by NIST and NSA will be identification of security tools that are needed in the Federal community. Thus NIST and NSA efforts will be focused on development of tools needed by the agencies and over the longer term, the security of our Federal systems will be improved further.

Coordination of NIST and NSA Activities

Your invitation letter asked that we address the relationship between the computer security and network security programs of the National Security Agency and the National Institute of Standards and Technology. NIST and NSA staff are closely coordinating on many of these activities. For example, both worked very closely with the Treasury Department in support of Treasury's Electronic Funds Transfer Authentication Program. They recently signed an interagency agreement on a joint project on computer network security directed at testing and verifying the interoperability of implementations of the secure data network system protocols. NSA has provided two secure data network protocols to NIST for inclusion in the Government Open Systems Interconnection Profile (GOSIP) project.

Other examples of NIST - NSA coordination include their announced intention to jointly review agency computer security plans, their cosponsorship of workshops on implementing the Computer Security Act, their cosponsorship of the National Computer Security

Conference and their joint establishment of a risk management laboratory housed at the NIST facilities in Gaithersburg, Md. NIST has begun drawing upon the technical expertise at NSA, and vice-versa.

It is essential that the two agencies closely coordinate their security activities. To do an effective job, NIST must understand and take maximum advantage of security tools and methodologies developed by NSA when they are applicable. We cannot afford to duplicate unnecessarily the expertise resident at NIST or NSA. At the same time, the nature of the information they are charged to help secure and the potential threats are often very different. The Act acknowledges these differences and provides a rational framework for separate, but cooperative work. For these reasons the two organizations are actively participating in each other's forums, participation that we encourage and support.

As I have outlined, we are actively moving to implement the Computer Security Act of 1987. We believe that the Act gives us a framework, and provides the momentum for the government to address the security of Federal computer systems, and we believe that the agencies have made a good start. We look forward to continuing to work closely with the Subcommittee on this important effort.

I would be pleased to answer any questions that you may have.

Mr. MCCURDY. Thank you, sir. What progress has been made in the identification of sensitive information systems in operation and under development?

Mr. PLAGER. That's difficult to give a global answer to, Mr. Chairman, because under the procedures that are in place, we will not actually know the systems that are identified as sensitive systems, until the plans themselves come in. As part of our guidance to the agencies in the preparation of their plans, that guidance requires that they identify the systems and fill out a substantial amount of detail for us, so that we understand what it is that they are describing, and why they concluded it had sensitive material in it. That will accompany their actual plans when they come in.

Mr. MCCURDY. That's January the 8th?

Mr. PLAGER. Yes, sir, that's the target date.

Mr. MCCURDY. Short of those plans, is there any progress for providing for security training within those agencies?

Mr. PLAGER. Yes, sir, that program is already underway and under the statute, the training program goes into effect within, I think, it's 60 days after OPM issued their initial guidance which has gone out. I believe training programs are to be underway this month.

Mr. MCCURDY. What is the status of the re-write of NSDD-145?

Mr. PLAGER. The National Security Council has that task, and is in progress on it. I understand they have not given us a particular deadline or date for issuance of the revised directive.

Mr. MCCURDY. We are going to have a change in Administrations, and actually your January 8th date will be just before being the final days of this current Administration. Is it the intent of the Reagan Administration that this re-write will be accomplished prior to his leaving office or the transition?

Mr. PLAGER. The Admiral——

Mr. MCCURDY. The Admiral wants to answer that question?

Mr. PLAGER. The Admiral suggests that it is NSA rather than NSC. My information is—well, I am sure it is one or the other or both.

In regard to your question, Mr. Chairman, I think it is widely understood that there is a need for revision to that directive. I don't think there is any question about this Administration's commitment to address that issue. I honestly can't say what the time frame within which that will be accomplished but I do know it is under review and perhaps the Admiral, when he is before you, will be able to expand on that.

Mr. MCCURDY. I am sure we will discuss that in more detail, but having wrestled with that on the floor I guess I was in a unique position, having during the time of this Act serving on all three of the Armed Services Committee, Science and Space, and Intelligence and I was getting it from all sides as to where this compromise would come out and we spent a lot of time with definitions of some pretty words. It was quite a process to get the compromise and the Act passed and we'd like to—and this was a major consideration within that.

Mr. PLAGER. I was not a player at that time but I understand what you are saying.

Mr. McCURDY. It is not always a fun game to watch. How would you characterize the working relationship between NIST and NSA, since you are in that perspective of being able to see both?

Mr. PLAGER. Yes, sir. I think that in fact that working relationship has turned out to be quite good, perhaps to some people's surprise but certainly not necessarily so. There had been prior relationships between those organizations and I think they have proceeded to carry out their assignments under this Act in a good faith and cooperative manner.

Mr. McCURDY. Do you believe there are problems remaining though?

Mr. PLAGER. I think there are still a few substantive issues that they are working on ironing out. Their Memorandum of Understanding is well along. They have set up their joint teams to work together in reviewing the plans and I think the over-all progress has been excellent. I am sure there are issues that always need some addressing but that is a coordinative activity that goes on in the Government all the time.

Mr. McCURDY. Have they reported to you as to the status of that MOU and whether or not there is a date, target date, for that?

Mr. PLAGER. I do not know of a hard date on that. I do know that they are very well along and that most of the issues have been resolved and that they are continuing work on getting final resolution.

Mr. McCURDY. We understand there may be some difficulty in resolving responsibilities related to cryptology in the scenario and I can't go into much detail.

Are you aware of such difficulties?

Mr. PLAGER. I think that is an issue that has not yet been fully worked out, is in the process of getting worked out. I have every confidence that NIST and NSA will be able to work it out but I can assure you that if they are not able to resolve the issue between them that OMB is prepared to mediate and to assist and to assure that that issue does get worked out.

Mr. McCURDY. Is the National Computer Security Center at NSA, which is a fine center. I've been through it.

I was very impressed by the capabilities there. Are they providing technical assistance to NIST and its role to develop security standards for several applications?

Mr. PLAGER. They are, sir.

Mr. McCURDY. Have you considered moving the National Computer Security Center or a portion of it to NIST?

Mr. PLAGER. No, not in any serious way. It seems to us that both NSA and NIST have complementary responsibilities that each of them must address in their own sphere and it makes sense to leave their resources and programs in place to address those issues and at the same time, since they are doing so well on a cooperative level there seems to be no need to disturb that.

Mr. McCURDY. Back to training. Are you satisfied with the OPM interim regulation?

Mr. PLAGER. OMB, sir, is never satisfied with anybody's regulation. [Laughter.]

Mr. McCURDY. You are in the right job, aren't you?

Mr. PLAGER. On a more serious note, yes, we are satisfied with the OPM regulation. It is an interim regulation. We must remember that the Act I think intentionally created a set of deadlines if you will that require that the logical steps could not be taken one step at a time as we proceed down the road, but a number of things had to be done in parallel and OPM proceeded to get that regulation out on the training program.

I am sure they have in mind and I know we will be having an opportunity later down the road to look at revisions to that, but they did their job. They got that out. We got the guidance started and we're quite pleased that this process is working effectively in parallel.

Mr. MCCURDY. I keep coming back—and we in Congress are never satisfied either—as to the milestone for submission of the plans, and you say January 8, 1989 is the date. The problem is that if they don't meet that date, there's not a lot of authority out there to crack heads at the last minute and you are going to have transition. Of course selection will be determined by then and so there may be a little more certainty at that time, but I am just curious how confident you are they are going to meet that milestone.

Mr. PLAGER. Well, I am confident, Mr. Chairman, that the new Administration will be as committed to implementing this Act as the current Administration and I think we will put every effort into assuring that the agencies do meet that milestone. I know of no reason why they shouldn't.

Some of them will no doubt have problems meeting it but I think the statute is clear and the Administration's guidance on it is clear, that they are to meet it.

Mr. MCCURDY. Well, I can assure you that since neither of the gentlemen on this dais have general election opponents and therefore we are already members of the next Congress, we intend to be here to ask those questions again and if you are still around——

[Laughter.]

Mr. MCCURDY [continuing]. We'll be holding you to that date on the January 8th deadline there.

Mr. PLAGER. I will look forward to the colloquy.

Mr. MCCURDY. Good.

Did you suggest to the Deputy Secretary of Defense that you consider the control of outlays for small business contracts related to the Computer Security Act, such as computer security training?

Mr. PLAGER. I am familiar with that issue, Mr. Chairman. The Secretary of Defense in putting the controls on outlays had to look at the whole question of defense outlays in a global environment in a global sense, and I am confident that in making his judgments about how to manage the department and the department's scope and condition he took into account a large number of considerations.

There were unfortunate consequences to individuals and individual programs but I am sure that in his over-all strategy he did the right thing for the country and for our fiscal condition.

Mr. MCCURDY. Are you a lawyer by chance? I am not sure my law school prof would have let me get away with an answer like that.

Do you really believe the Secretary of Defense made the right decision there and are you going to advise—or the Deputy Secretary—of the difficulties that he's caused to small businesses wishing to offer computer security training services to Defense?

If they don't fall under these criteria, I mean who—and in the Armed Services Committee, that is a third of the Federal budget. I would like to see that the largest agency complying with the Act and certainly even though they had difficulty in generating business for small businesses they tend to get locked into the larger.

We'd like to see that opportunity exist.

Mr. PLAGER. One of the responsibilities that OMB has in Government is to look at the behavior of individual agencies, the way in which they carry out their particular programmatic responsibilities and try to look at it more globally, more across the Government.

In this case I find myself in the peculiar position of having a specific programmatic responsibility, carrying out Computer Security Act responsibilities as well as Information Collection Act responsibilities and I am a little bit reluctant to argue that that responsibility should supercede the broader responsibilities that the Secretary has for management of his program.

If it is the Chairman's wish, I will of course be sure that they have been sensitive to the impact of this on computer security issues and hope that they have taken that into account in making their decisions. If that would be helpful, I would be glad——

Mr. MCCURDY. Well, when we had a hearing—and I understand the Department's difficulties right now—to give you an example, when we had Mr. Taft before the Armed Services Committee regarding the Taft memo on the freeze I asked him—and that was back in July, I think—I said, Mr. Secretary, can you tell me how much money as of today's date the Department of Defense has obligated or spent for the first six months of the year and he turned to his legion of aides behind him and they got out the big black books and they were thumbing through and they huddled for a minute and then they came forward and said plus or minus $20 billion?

So I am sure there is a green eyeshade guy downtown at OMB that makes you all feel real good, real comfortable, but it doesn't set too well up here. It does raise some concerns. I understand the difficulty of knowing how much—I am not sure I understand the difficulty of knowing how much they have obligated, but it certainly has wreaked havoc in trying to implement this plan.

We would like to see a little more control and perhaps a conversation would be welcome.

I was going to ask a question about the computer viruses perhaps the Admiral would like to discuss what steps they have taken within his agency to prevent those things, but how much of a threat does the Adminstration actually see this and what actions do you think are being taken to prevent it?

Mr. PLAGER. The information is not wholly complete I think or such that we can accurately describe all aspects of the threat. To some extent the threat is indeed more of a threat than a reality, which is not to say we shouldn't address it.

My understanding is that the threat is as much from inside and as much from inadvertence and error as it is from—at least on the civilian side of this, I am not now talking about a national security

issue—as it is from outside efforts to come in and wreak havoc with our systems for either personal gain.

Much of this computer virus business apparently stems from just maliciousness.

Mr. MCCURDY. We have cases where we have had disgruntled employees walk in to classified facilities in California and kill people because a woman did not accept his advances. We have had people walk into post offices in my state of Oklahoma and gun down people because of their particular grievances. If they are willing to do that, does it not appear to be a likely threat that a disgruntled Federal employee who certainly has a better understanding of computers than I do to go in and gum up the Social Security computers which are a pretty good sized network or some other agency—not even considering the national security implications but civilian agencies.

What would happen if they got in OMB's computers?

Mr. PLAGER. It would probably help them. [Laughter.]

Mr. MCCURDY. Probably help? Like a tornado in Cleveland.

Mr. PLAGER. Well, the scenario you describe, Mr. Chairman, is certainly there and it is certainly a possibility.

To some extent I think we have to acknowledge that just as attacks on the President's life occur despite all of our efforts to prevent them, to some extent I think we have to acknowledge that there are real limits in a democracy or even in a functioning government as to how much you can control and ensure and protect the daily operations of the Government, whether it is through computers or technology, whatever.

To the extent we can, where we can identify a real risk we ought to do whatever is necessary physically or mechanically or however to control that risk. But I think on balance when you look at the totality of systems and at the totality of databases and processes that go on in the Federal Government, the larger risk is not that kind of occasional violence. As I say, against that occasional violence I am not sure that you can actually ever be 100 percent protected.

Mr. MCCURDY. Well, I am not suggesting that we could be. I am not sure a cost benefit analysis would indicate that we should take the steps necessary to achieve that. However, from my experience in the classified arena there are checks as to how much access a person has to the totality of a system or totality of a block of information, whether it be need to know—you know, there are the checks and balances there.

In the civilian arena those people that have access to the total system, do they receive—perhaps in the development of your training schemes perhaps they should be given special training or there should be some checks as to the qualifications of the people or their status, whether or not they should have access and whether or not they are keeping the best interests of the Government in mind.

Mr. PLAGER. That, of course, is the wisdom of the Act, which I believe you were one of the major proponents of. What the Act says is that each agency should assess the nature of the risk and the kinds of problems they should anticipate with regard to the various major systems and come up with a security plan that is tailored to that system.

That was a very sensible way to go about it. There may, indeed, be some systems where the nature of the problem is the kind you're describing to the point where you've got to have a really carefully controlled environment, and maybe other systems where training and awareness within the existing security mechanism may be enough. And we can tailor—hopefully the agencies will be proposing plans that will tailor their cost benefit concerns through those kinds of situations.

Mr. MCCURDY. I know the gentleman from Florida would agree that there's probably not a more life-threatening scenario to a member of Congress than to have Social Security checks stopped. I would like to ensure that all necessary steps are taken to protect. Probably more in his district than mine.

Mr. PLAGER. Well, I'm a Floridian myself, so I understand the problem.

Mr. MCCURDY. The gentleman from Florida, of course, has been integrally involved the development of this Act and overseeing the implementation and even though I try to inject some humor, this is a very serious measure and the Chair always likes to thank Mr. Lewis for his support and cooperation and due diligence on these issues and I recognize him for as much time as he might consume.

Mr. LEWIS. Thank you, Mr. Chairman. I don't believe I have too many questions. I think you did a pretty good job. I noticed that in your report, Mr. Plager, that you referred to the GAO report in May and I just wonder why it takes so long, even though you're coming up with a plan, in order to put the security measures in place in these various agencies, such as OMB.

The reason for the Act was because of the lack of security measures. So it would seem to me the mere fact that the Congress worked toward a legislative solution to this, that the agencies would have taken the initiative prior to the enactment of the Act and moved ahead. Do you feel that the agencies are doing this now or are we going to wait until we get an overall glorious plan and then we'll put it in phases and take the next 20 years to get it in place?

Mr. PLAGER. Yes. I think that's a good question, Mr. Lewis. I think we tend sometimes to think that the world was just created on some particular issue. But in fact, in this case, the concern with security, information security, has been in front of the agencies and in front of the government now for some number of years and, in fact, there has been guidance put out by the old National Bureau of Standards and other parts of the Federal system that have been designed to make us all conscious of the problems of computer security well before this Act was put in place.

I think there are a number of agencies that already have plans in place, programs in place for dealing with computer security. We know, as a matter of fact, that when we have reviewed and approved the putting in place of some of these big systems that there have been incorporated in those systems a variety of security mechanisms and approaches.

So that's already being done. I think what the Act is doing is to both raise everyone's awareness, including those who have been paying attention, and creating an awareness in the minds of agencies that have not thought of themselves as subject to these con-

cerns. So that we now have a concern government-wide. But I think it would be a misunderstanding to think that a lot of this activity has not already taken place because of that.

Mr. LEWIS. That's good to hear. Mr. Chairman, I don't have any questions. I think you covered it substantially. I do have an opening statement that I would like to have inserted in the record.

Mr. MCCURDY. Without objection, it is always welcome. Thank you, Mr. Plager, for your testimony this morning. We will be watching as the January 8 date comes closer and appreciate your interest and involvement in this issue.

Mr. PLAGER. Thank you.

Mr. MCCURDY. Our next witnesses are Admiral W.O. Studeman, who is the Director, and James Hearn, Deputy Director for Information Security. Admiral?

STATEMENT OF REAR ADMIRAL W.O. STUDEMAN, U.S. NAVY, DIRECTOR; DR. JAMES J. HEARN, DEPUTY DIRECTOR FOR INFORMATION SECURITY, NATIONAL SECURITY AGENCY, ACCOMPANIED BY PATRICK R. GALLAGHER, JR., DIRECTOR, NATIONAL COMPUTER SECURITY CENTER

Rear Admiral STUDEMAN. Good morning, Mr. Chairman. This is my first appearance before this Committee and I have submitted a formal statement for the record and I'm not going to repeat what's contained in that statement.

I'm new at the National Security Agency. I've been on board for seven weeks and this is a new subject for me as an intelligence professional. So basically I've come to learn and observe here at this session dealing with this very important topic. I'd like to say at the outset that—the first thing I'd like to say is I'm deeply impressed with the National Security Agency's technology and level of commitment to the subject of information security, including computer security, and I've tried to study the issues related to the National Security Act with great interest since my arrival.

As the Former Director of Naval Intelligence, I was responsible for dealing with some severe security problems in the Navy, specifically Walker-Whitworth cases, Pollard, and a litany of others. I personally am doubly committed to the subject of ensuring that security is achieved at all levels of the Federal Government because I have obviously experienced the consequences of poor security.

I'd like to introduce Dr. Jim Hearn, who is the new head of the Information Security Division at NSA which, as you're aware, is basically half of the National Security Agency's mission. And also with us today is Mr. Pat Gallagher, who heads up the National Computer Security Center, and he's here obviously as a technical advisor if we get into subjects like computer viruses and things like that where you want some substantial detail.

One year ago yesterday, Mr. Chairman, you came out and gave a speech at the 10th National Computer Security Conference in which you indicated that issues put forth by this important piece of legislation extend far beyond mere turf battles amongst competitive government agencies. In fact, you stated specifically that an unusually broad private sector constituency ranging from the banking community to university libraries to civil libertarians felt

it had a stake in the outcome and that this bill would meet the needs of this constituency and still achieve the basic purpose, namely to improve computer security at the Federal establishment. It's been a challenge and it's a compromise and it's far from perfect.

My view basically as the Director is that NSA has made impressive progress in a whole litany of areas, and let me elaborate a little bit on some of those. Work in metrics, our word for standards, support to the training requirements, conferences on the subject, work in networks, network interoperability, database management, operating systems, hardware transfer ability and architecture, risk analysis and management, personal data security information exchanges on functional security devices, integrity of software, a whole lot of other issues.

By the same token, we still have some details to work out on certain aspects of the law which enjoin us to specifically, quoting from the law, avoid unnecessary and costly duplication of effort and have standards and procedures which are consistent and compatible across Federal systems where feasible. I am really optimistic that we can work out the final details of the split responsibilities between NIST and the National Security Agency, and that this will be embodied in the final version of the memorandum of understanding.

And that we can also work within the government, the National Security Council, and others to ensure that we also have an ecumenical NSDD that addresses both the defense as well as the government security issues and incorporates, in essence, what's contained in the law in a new NSDD.

So our role basically we see is one of support that goes beyond our interest obviously in ensuring that information security exists for classified systems and we intend to carry out that mission to the letter. I would like to recommend here, since you've already brought it up, that the complex subject of cryptography is really a more appropriate subject for a closed session, which we strongly support.

At this point in time, I'd like to turn over the mike to Dr. Hearn, who is again the head of Information Security for the National Security Agency.

Dr. HEARN. Mr. Chairman and members of the Subcommittee, I am pleased to appear before you today to testify on NSA's activities to assist in implementation of the Computer Security Act of 1987. As Admiral Studeman mentioned, we are accompanied by Mr. Pat Gallagher, who is Director of the National Computer Security Center.

It is our view that there are several examples which attest to the good cooperation that exists among the organizations present today to implement provisions of the Act. We have attempted to support those agencies who have primary implementation responsibility by providing information on our computer security training and awareness experience and by assisting and drafting guidance to the Federal agencies so they may formulate the security plans required by the Act.

With NIST, we will be jointly reviewing those plans when they are submitted in early 1989. We are now working with NIST and

OMB to determine how big this job will be and to dedicate the necessary resources to provide timely comment to the agencies involved.

We will also appoint a senior NSA official to serve on the NIST-established Computer Security and Privacy Advisory Board. We understand that the invitation from NIST to participate in this activity has been sent to us.

I would like to turn to our efforts to provide technical assistance to NIST. Over the years, NSA and NIST have conducted joint study and research projects on a wide range of computer security topics. We have also jointly sponsored the annual National Computer Security Conference. This year will mark the 11th such conference.

With the enactment of the Computer Security Act, it is clear to us that this relationship will continue to grow. Two agencies cannot properly advance the state of computer security across government without close coordination of programs and strategy. We at NSA, must stay aware of NIST's plans in setting computer security standards for protecting sensitive information so we can ensure our activities in such areas as technical product development and evaluation, are compatible with NIST's standards.

Conversely, NIST needs to remain aware of ongoing programs within DOD and NSA which may help provide solutions to the problems NIST faces in the sensitive government and private sector environments. We are sharing technical information with NIST on our R&D efforts, which are directed to DOD and intelligence community needs, and which may prove beneficial to the needs of the rest of the government. With this in mind, we have provided to NIST, a listing of all technical guidelines completed—those currently being written, and those planned through 1990.

We have also provided information on network interoperability standards, a summary of training and awareness efforts, and a list of technical topics that will be briefed to NIST. With your permission, Mr. Chairman, I would like to submit these documents for the record at this time.

Mr. MCCURDY. Without objection, so ordered.

[Information to be furnished follows:]

UNITED STATES DEPARTMENT OF COMMERCE
National Bureau of Standards
Gaithersburg, Maryland 20899

April 4, 1988

Mr. Patrick Gallagher
Director, National Computer Security Center
Fort George G. Meade, MD 20755-6000

Dear Pat:

In accordance with the provisions of PL 100-235, I would like to formalize our interactions to improve the computer security posture of unclassified information processing in the Federal government. I hope these interactions will be beneficial to both our organizations but especially to the intended users of computer security methods.

We would like to begin drawing upon, and using the experience and products of your organization in helping to meet our goals that were established by PL 100-235. We have analyzed the Law and are initiating several activities that are very important in meeting our objectives. I will not present them all in this letter but will only outline several that we feel have high priority. The information that we need is then summarized for each of these activities.

First, we would like any written material regarding computer security awareness and training that you have developed that is appropriate for protecting unclassified data. These include course descriptions, outlines, objectives, visuals and texts or textbooks. We would also like your recommendations of instructors or instructional organizations that could be utilized in this activity.

Second, we would like an annotated bibliography of your technical guidelines that you feel we could draw upon in developing training materials, interoperability standards and functional profiles (interoperable subsets of generic standards). The bibliography should include, if possible, the scope, approach and applicability of each guideline. If additional guidelines are in preparation or are planned, we would appreciate a description of these. My staff has been interacting with Eliot Sohmer on these but this request is to formalize this activity.

Third, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, issued a memorandum on July 2, 1987, to the effect that information resulting from the Secure Data Network System Project (SDNS) should be made available for use in the Government Open Systems Interconnection Profile (GOSIP) project. The GOSIP document is proposed as a Federal Information Processing Standard and will first be issued in 1988, with revisions intended to be issued annually thereafter. Dennis Branstad has actively participated in the SDNS project and has been informally assured that the SDNS documentation will be made public in May 1988. I would like you to verify this timetable for delivery of this information. We would also like to know if all of the documentation will be made public. Our goal is to use the products of this activity as much as possible in the GOSIP project.

Finally, we would like to receive briefings or to hold discussions on technical topics that may require research in order to develop needed standards in the near future. These include personal authentication techniques and digital signatures for electronic documents. Again, we would like to use the results of your on-going projects to meet our objectives. We do not want to duplicate your research activities. However, the information must be unclassified and then must be publicly reviewed in order to satisfy our needs.

I look forward to continuing these interactions with you and your organization on these activities. Please call me if you have any questions.

Sincerely,

James H. Burrows
Director
Institute for Computer
Sciences and Technology

NATIONAL COMPUTER SECURITY CENTER
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: C-071-88
20 April 1988

Mr. James H. Burrows
Director
Institute for Computer
Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

Dear Mr. Burrows: Jim

I am responding to your letter of 4 April 1988 which asked for our assistance in providing information on computer security awareness and training, technical guidelines, the Secure Data Network System (SDNS) project, and technical briefings which may require research in order to develop needed standards.

As I mentioned in our telephone conversation last Thursday, we are delighted to assist in any way we can. Exchanges of information, such as this between our organizations can only enhance our respective efforts in improving the security and privacy of sensitive information in Federal computer systems.

I have had my staff pull together several packages for you. Enclosure 1 contains the awareness and training information you requested.

I believe the SAISS Education, Training, and Awareness Working Group is an excellent resource you could draw upon to meet the requirements of Public Law 100-235. The group is chaired by the Office of Personnel Management's representative to the SAISS, Harold Segal, Chief, Policy Oversight Branch, Office of Training and Development, and is the best heterogenous mix of individuals from across the federal government focused on computer security education, training, and awareness. I've attached a membership list for your perusal (Enclosure 2).

As you may recall, the SAISS charged the group to develop an integrated approach to computer security education, training, and awareness throughout the federal government; to develop a briefing to heighten the awareness of cabinet-level officials; and to develop a means to hold management more accoutable for their actions.

The group has held three meetings, the results of which are reflected in the attached minutes (Enclosure 3). Please note that the minutes of the 9 March 1988 meeting include the group's initial effort to identify the categories of individuals/ functions for which training is needed; the training needed for each group; and the risk assessment model which should be used.

Enclosure 4 contains the annotated bibliography of our technical guidelines to help in the development of training materials; the interoperability standards and functional profiles; the scope and description of each guideline and a list of guidelines that are planned.

With regard to the Secure Data Network System (SDNS) Project, I am quite pleased with the results so far and particularly with the excellent working relationships that have been developed among Dennis Branstad, the contractors, and our personnel. A number of SDNS specifications have reached an initial release status and are being used by the contractors to implement the protocols. Several of these specifications draw heavily from our FIREFLY Key Management Technology which is releasable only to U.S. Government activities and U.S. Government contractor personnel. However, early in April, we did send two specifications, Security Protocol 3 (SP3) and Security Protocol 4 (SP4), to the appropriate organizations here at NSA for review and concurrence that the documents are unclassified and suitable for inclusion in the Government Open Systems Interconnection Profile project. We expect the review of these documents to be completed during May 1988.

As requested, we have identified several technical topics to brief for your information (Enclosure 5). Each may require research in order to develop needed standards. I have asked Dr. Pinsky, my Senior Scientist in the Research and Development Office to take the lead on this. We will plan to brief two or three topics starting in May either at NBS or here, as convenient.

Please let me know if the packages we have prepared provide you the necessary information. If further information is needed please give me a call.

Sincerely,

PATRICK R. GALLAGHER, JR.
Director

4 Encls:
a/s

Dr. HEARN. There are numerous other technical areas of current and potential NIST/NSA cooperation. Risk management, functional security devices and a technology base for personal data security devices are just a few. In your letter inviting us to appear today, you asked for information on several specific computer and network security programs at the National Computer Security Center, which might support the standards programs at NIST.

This information is included in our statements for the record. Since this is quite technical, I would prefer not to discuss those programs in detail at this time. I would like to note, however, some of these programs are still in the early stages of development, and documents published by the National Computer Security Center, such as the Trusted Network Interpretation, are still in draft form and have been distributed for comment.

We will be coordinating our efforts closely with the NIST to keep them informed. In some areas, we may be able to develop both classified and civil versions of technical initiatives. In other cases, such as the civil use of the orange book, we believe the technical basis of that document can be of use to NIST as it considers how best top meet the needs of the civil sector.

We understand the importance of having a single set of federal guidelines, Federal Government Guidelines, to which the American industry can build computer security products. We feel that NSA and NIST can work together effectively to accomplish this. In closing, I would like to repeat NSA's commitment to sharing our technical excellence with NIST to ensure that the goal of furthering the security of our nation's computers and computer networks is met.

As the depth and breadth of our joint activities grow, we are confident the mission needs of the two organizations can be accommodated. Thank you for the opportunity to speak to you today. We would be happy to answer any questions you might have.

[The prepared statement of Dr. Hearn follows:]

90-130 O - 89 - 2

STATEMENT

BY

DR. JAMES J. HEARN

DEPUTY DIRECTOR FOR INFORMATION SECURITY

NATIONAL SECURITY AGENCY

CONCERNING

IMPLEMENTATION OF THE COMPUTER SECURITY ACT

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 22, 1988

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

Thank you for the opportunity to appear before you today to discuss the status of implementation of PL 100-235, the Computer Security Act of 1987. In August of this year, I became the new Deputy Director for Information Security at the National Security Agency. As you are aware, both Admiral Studeman and I have just recently assumed new responsibilities, and are looking forward to the challenges and opportunities that await us.

I would like to describe for you today the areas and extent of the National Security Agency's participation in efforts to implement the Act, and more specifically, our collaboration with the National Institute for Standards and Technology (NIST) in support of its new role as lead agency for protecting sensitive data in government computer systems.

Let me begin by saying that the level of cooperation amongst the agencies involved in implementing the provisions and intent of this legislation is impressive. Under OMB direction, the group, composed of OPM, NIST, and NSA, has demonstrated an ability and a desire to work together to get the job done. This has led to joint decisions regarding training and security plan requirements and made it possible for the OMB working group to provide guidance to Federal agencies and meet the rather short deadlines imposed by the

Act. NSA, in particular the National Computer Security Center, is taking its supportive role seriously by providing expertise in various areas as requested.

At the time this legislation was introduced, NSA raised concerns over the potential harm to the government's information security effort which could arise from a split in authority between NSA and NIST. Those concerns stemmed primarily from our belief that the government needs a single set of standards to which American industry can build the products we need to protect government computer data. I am pleased to report we are working closely with NIST to ensure that standards for the classified world and the sensitive data world for which NIST now has responsibility, will indeed be compatible. We are hopeful our two agencies will succeed and that we will avoid sending mixed or conflicting signals to industry.

NSA has moved ahead in carrying out its role in implementing the requirements of the Act. We were pleased to be able to participate in the interagency working group headed by OMB and consisting of NIST, OPM, and NSA, which was formed to assist in the development of the computer security training regulation and guidance. We have also assigned personnel to support the OMB data call for agency security plans and will be jointly reviewing these plans with NIST. Several NSA personnel participated in the July workshop at NIST which was held to

explain to federal agencies the training and security plan provisions in the law. We anticipate an ongoing effort to support OMB, OPM, and NIST until all of the requirements are successfully implemented.

NSA is also required by the law to be a member of the Computer Security and Privacy Advisory Board under the Department of Commerce and NIST. We look forward to this opportunity and are prepared to proceed.

Turning now to the growing relationship between NIST and NSA, as both agencies have previously testified, we have enjoyed a longstanding cooperative relationship with NIST. In the past, the two agencies have conducted many joint studies and research projects. In addition, this October will mark the 11th Annual National Computer Security Conference hosted jointly by NIST and NSA.

With the enactment of the Computer Security Act, it is abundantly clear to us all that we cannot properly advance the state of government computer security without close coordination. We at NSA must be aware of the plans of NIST in setting computer security standards for protecting sensitive information in the civil sector of government so we can ensure that our activities in product evaluation and other technical areas are compatible with those standards. Conversely, NIST needs to be aware of ongoing programs within DoD and NSA which

may help provide solutions to the computer security related problems in the sensitive government and private sector environments.

The Computer Security Act requires NIST to draw upon the technical assistance and work products of NSA as it deems appropriate for use in its mission of protecting sensitive government data. While the National Computer Security Center computer security research effort is directed at DoD and Intelligence Community needs, many benefits may be derived from our research which are applicable to the rest of the government and the private sector. As such, NSA's Information Security Organization has provided NIST with a wide range of information on its technical programs and publications, and is working collaboratively with NIST in several areas.

This includes:

--a summary of the ongoing computer security educational, training and awareness efforts at NSA and within the National Telecommunications and Information Systems Security Committee (NTISSC) structure. NSA, for example, has an on-line computer system called DOCKMASTER that offers access to a wide range of areas covering information security activities. The NCSC recently agreed to work with NIST to see how this system can be used in support of NIST's awareness activities. Another good

example of a collaborative effort with NIST is an upcoming seminar (May 1989) to be conducted under the auspices of the National Engineering Consortium, an established meeting ground for industry and academia since 1944. The NSA Assistant Deputy Director for Information Security and the Director of NIST's National Computer and Telecommunications Laboratory have agreed to a request from the Consortium to co-chair a forum on U.S. Government Information Security Policy, a first of its kind..

--a bibliography of published technical guidelines to aid in the development of training materials. This includes publications completed, currently being written and those planned through 1990;

--networking protocols suitable for fostering network interoperability;

--suggested technical topics to be briefed to NIST in support of potential new standards development. The NCSC has presented technical briefings to NIST on such topics as computer viruses and data integrity. Next week, NIST will be sending personnel to participate in the first meeting of the NCSC Data Integrity Working Group.

I have taken the liberty of submitting for the record copies of a selection of materials provided to NIST.

The area of risk analysis is important to system managers in assessing their overall security posture and needs. In the associated area of risk management, which is critical to maintaining a system security posture, we can point to a record of technical and programmatic cooperation between NIST and the NCSC of which both agencies are very proud. We have jointly established a Risk Management Laboratory housed at the NIST facilities in Gaithersburg, MD, to provide both user support in risk analysis and a joint agency R&D facility for risk analysis techniques. The Risk Management Lab, with associated expertise, is available to government agencies to aid in performing initial and follow-on risk assessments of their systems. NIST will also use the lab to further advance the state of the art in risk analysis in the broad sense which includes the full spectrum of risks to computer systems (fire, theft, flood, etc.), while the NCSC supports and augments that research with concentration on risk analysis aimed at the challenges of multilevel security systems and the aggregation of classified information. The two agencies have also jointly hosted a risk analysis workshop and continue to cooperate closely in assessing various candidate methodologies for conducting automated risk analysis. When further research on new and emerging methods of risk management are available, future joint workshops will be sponsored.

The NCSC and NIST have also exchanged information on a variety of functional security devices, e.g., dial-back modems, "smart cards", and retinal scanners for user identification and authentication. Discussions are currently underway regarding the establishment of conformance testing for these types of devices by NIST's National Computer and Telecommunications Laboratory.

We have agreed to assist NIST in developing a technology base for a personal data security device for personal authentication, data integrity, and data confidentiality.

Finally, NSA, NIST, and the Department of the Treasury have signed a Memorandum of Understanding (MOU) in support of Treasury's Electronic Funds Transfer (EFT) Authentication Program. The MOU defines NSA support to Treasury for NSA certification of equipment meeting Treasury's EFT criteria. One product has been certified thus far, and two more are being evaluated.

As I mentioned earlier, this fall will mark the eleventh time that NSA and NIST have jointly sponsored the National Computer Security Conference. We were pleased, Mr. Chairman, to have you as our keynote speaker at the conference last year. I am equally pleased that this year Congressman Tom McMillen, also a member of this Subcommittee, has graciously agreed to be

our keynote speaker. We appreciate the support you have shown for this conference. This year we expect over 2000 people from government, industry, and academia to attend, and I would like to take this opportunity to invite you and your colleagues and staff to attend as well.

In your letter inviting us to appear at today's hearing, you asked for specifics on how the computer and network security programs at the National Computer Security Center can support the security standards program at NIST, and more particularly, our specific plans for supporting the security standards program at the NIST in the development of civil versions of: (1) the Secure Data Network System (SDNS), (including NIST public key and key management standards and using the NIST Data Encryption Standard as the encryption standard for SDNS); (2) the Trusted Computer System Evaluation Criteria (hereinafter referred to as the "Orange Book"); (3) the Trusted Network Interpretation (TNI) of the Orange Book, including assuring that SDNS capabilities are compatible with and directly related to the TNI; and (4) the forthcoming Trusted Database Interpretation for the Orange Book.

This is a significant agenda and we have only begun to embark on some of the projects; thus, I will briefly describe major work underway between the two agencies.

In 1985, NSA initiated contracts with ten industry leaders to assist in the design of cost-effective, user-friendly and fully interoperable approaches to secure data as it travels through a network. This effort was called the Secure Data Network System (SDNS). NIST and the Defense Communications Agency have since joined NSA and its contractors in several aspects of this project. As a matter of fact, officials from the NIST have been full partners since 1986 in a working group which is responsible for security protocols in the SDNS. To that end, NSA recently released two SDNS protocols to NIST for inclusion in the Government Open Systems Interconnection Profile (GOSIP) project. As you are aware, GOSIP is expected to become the preferred protocol standard for government systems, and will most likely become an international standard as well.

NIST and the NCSC recently signed an interagency agreement on a joint project on computer network security directed at testing and verifying the interoperability of implementations of the SDNS protocols. NIST will, in conjunction with the NCSC, establish an Open Systems Interconnect (OSI) laboratory and design and develop a demonstration system showing interoperability of devices implementing the SDNS OSI protocols.

Since its introduction at last year's joint NIST/NCSC Computer Security Conference in Baltimore, we have distributed

more than 10,000 copies of the Trusted Network Interpretation (TNI) of the Orange Book. Experts around the nation are reviewing it, and subsequent editions will benefit greatly from the comments that we receive. I am pleased to say that a number of U.S. vendors have responded to the TNI by building products to its criteria, and that we are evaluating several network security products as part of the Trusted Product Evaluation Program (TPEP).

The Trusted Database Interpretation of the Orange Book is being designed to encourage the commercial development of trusted database management systems, and to enable the evaluation of those Data Base Management Systems in a way that will be compatible with products evaluated against the Orange Book and the Trusted Network Interpretation. Our intention is for one version of the Trusted Database Interpretation to be applicable to both the DoD and the civil sector. We believe that the various requirements being worked into the Trusted Database Interpretation will result in the production of database management systems that can be trusted to protect all types of information.

Use of the Orange Book as a foundation for civil sector computer security is under discussion. In the meantime, NIST supports civil sector use of products that have been evaluated by the NCSC against the Orange Book criteria, particularly those products with a C2 level of trust.

NIST recently requested that we develop a set of compliance tests whereby any user or vendor could test the security of a system designed to meet a C2 level of trust. While we work to satisfy this request, NIST has asked us to continue with all our ongoing evaluations of C2 level systems.

In addition to the specific information that the committee has asked that we provide, I would like to take the opportunity to describe the breadth of research and development activities conducted at the National Computer Security Center. Our R&D work is primariliy directed towards three "product lines" involving products for secure networks, secure database management systems, and secure computer operating systems and hardware architectures. In each of these product areas we have aggressive programs which will result in the near-term availability of products at the highest levels of trust. Periodic information exchanges regarding these developments are conducted with NIST in order to consider their potential applicability to the public sector.

In the secure computer systems area we are pursuing a revolutionary approach to incorporating security features as part of the hardware base of the machine. An important feature of this approach is that it is readily transferable from one hardware base to another and can be applied to existing non-secure hardware systems, thereby saving the

customer the expense of replacing his existing equipment to achieve security. Our solution, which is aimed at the highest level of trust, the A1 class, holds the promise of allowing computer security features to become truly ubiquitous for a wide variety of classes of machines. A prototype of this capability will be demonstrated next March.

We have made significant progress in applying computer security to database management systems. Such systems are implemented either as part of a computer's software system or as a specialized database machine. We have made breakthroughs in introducing security features in both approaches, and C2-level products are expected by the year's end.

Various security problems surface when connecting stand-alone workstations to a network. The current lack of terminals capable of simultaneously protecting different levels of sensitive material contributes to this problem. Our Multilevel Secure Workstation program addresses this deficiency. Through this program, high performance workstations capable of operating at the B level of trust will be available within the next six months.

Beyond these product-focused R&D efforts, our researchers have devoted considerable resources to improving the process by which NIST and NSA implement secure systems. To this end we have begun to marry the fairly mature discipline of software

engineering with the formal mathematical methods employed previously to "prove" the security of systems. This has been a fruitful marriage and the concept along with the introduction of "expert system" technology will allow us to make considerable improvements in what is now a largely manpower-intensive process.

All of the above efforts are applicable to the broad community, i.e., both classified and sensitive, of information processors. By providing the results of our research to NIST, we believe all sectors of the user community requiring protection are being served.

As has been our goal since the inception of the NCSC, we will continue to work for the furtherance of security for our nation's computers and computer networks. We are committed to sharing our expertise with NIST to ensure that this goal is met. As the depth and breadth of our joint activities grows, we are confident that the resources of both agencies will continue to effectively complement each other, and that our organizations efforts will remain compatible.

I thank you once again for the opportunity to address the Subcommittee and would be happy to answer any questions that you have.

Mr. MCCURDY. Thank you, Dr. Hearn. Admiral, I know that I had spent a lot of time with Admiral Burkhalter and General Odom on these issues, but the engagement was a rocky one. I think the marriage, now that it's been consummated, is hopefully going better than expected. I picked that up in your comments. Is that an accurate assessment?

Admiral STUDEMAN. I think I have to be optimistic about what can be achieved.

Mr. MCCURDY. The honeymoon has been all right. Maybe that's better.

Admiral STUDEMAN. I think we still have some issues to work out, and I wouldn't want to minimize the complexity of those issues, but I'm optimistic that we're going to be able reach a fairly rapid closure here on those issues.

Mr. MCCURDY. I asked Mr. Plager about the dates on the NSDD and the re-write and do you have any targets, any milestones on that?

Admiral STUDEMAN. Yes, sir. I think that beyond what's been said, I guess it's part of our process that we undergo changes in Adminstration. Obviously, we've got to be, in terms of the kind of things that we've set for ourselves in pursuit of the law; we have to be independent of those kinds of things, including doing things like drafting revised National Security directives that relate to this important topic of computer security.

Mr. MCCURDY. Does that re-write, though, does that not require acceptance by the Administration?

Admiral STUDEMAN. Absolutely, and we'll have to deal with whichever Administration.

Mr. MCCURDY. Wouldn't it be better to deal with the Administration that was in office during the time of the Act, than to wait for whatever the next Administration—so, wouldn't that itself be a milestone?

Admiral STUDEMAN. That would certainly be desireable. Certainly, there's a great base of knowledge and this Administration has been through a great deal of education and association with this topic. It would be desireable if we could pump out an NSDD that, in fact, deals with this topic in the more ecumenical manner, and gets past the issues that you were concerned about in the earlier testimony on this particular subject when I know NSA was, in fact, having difficulty with their particular position on the law.

Mr. MCCURDY. I think it's the position of this Subcommittee and certainly the Congress that we'd like to move as rapidly as we can on this law and the implementation. Again, not trying to glamorize, but when we were doing the Act, it was hackers. When we went through the Center, there were some pretty graphic examples of how many of our important networks were tapped into. Yet today, we are seeing—the more the virus makes the front page cover, and I'm married to a psychiatrist so I hear this a lot. The more publicity that's given to those problems, the more likelihood, or the greater the likelihood that someone may actually attempt them.

It's like mass suicides or something. The risk, I think, increases the more that the information is available. It's like building a bomb in your basement. Maybe somebody might see the plans, or

you know, get some information on how to do that, and I think we need to move as rapidly as possible to ensure the security and safety of our computers.

Admiral STUDEMAN. As you are probably aware, Dr. Bob Morris, who is the technical director of the National Computer Security Center is mentioned in that article.

Mr. MCCURDY. That should be the premiere center in the United States, maybe in the free world, on how to deal with those kinds of issues. No one has ever questioned the expertise or the ability of the people involved. The question is, how do we get it out of one building and throughout the Federal Government. I mean, it's great to have—it's a beautiful facility and it's a great group of people and they've got a lot of fine minds, but if you don't get it out there into the local offices or, you know, the other agencies, it doesn't do us a darn bit of good.

That's our concern. We just want it implemented. Get it out of the ivory tower into the workplace, and that's our major concern.

We have a vote for which we probably should take a short ten minute break—five minutes if possible, and return. I'll yield then to the gentleman from Florida and the gentleman from Maryland, who, by the way, is going to be the speaker at this year's computer conference. I'm sure he's going to do a better job than last year's speaker. We'll take a short break here.

[Brief recess.]

Mr. MCCURDY. Pat, it is good to have you here.

Mr. GALLAGHER. Good morning.

Mr. MCCURDY. I was going to recognize my colleagues but they haven't made it back from the vote. While we have you at the table, I might ask if you could give us a little more information as to how you think you can protect against things such as the virus and the other illegal entries.

Mr. GALLAGHER. I would be pleased to. Let me separate the problem particularly of the virus into the work that we have done and what we think we can do. We have been looking at viruses as somewhat of an academic curiosity to understand how that operated in the machine. Obviously, about seven, eight or ten months ago we put more energy into that because it became obvious that was a problem of some importance.

We went to places like University of Delaware and other universities that were reporting viruses, identified ourselves, said we were interested and we would like to share with them what we knew and find out from them what they knew.

What we tried to do was to codify viruses or to erect a taxonomy of viruses. Some are more pernicious than others. We think we have done that and put them into four categories from very simplistic to very complex.

That research goes on as more viruses continue to emerge and as we do some of our own work in just thinking through the problem.

Secondly, we thought it would be an useful contribution to society to look at products on the market that do something about viruses. We looked at things called a flu shot, doctor data and other products. There is a whole great proliferation of those products out. We thought it would be useful to look at them, see what they did and see what they don't do, see which in the taxonomy they take

care of and which they might not and promulgate that information.

We also thought, in coming to your earlier point, to collect knowledge within the Center and not to disseminate it is not a very useful thing. We put together a briefing on the virus that we have shared with the Federal community through the instrumentality of the committees that have been set up under the NSDD, with the defense community and with the intelligence community. Specifically with my brothers at NIST, for their use in whatever manner they wished and to promulgate that information.

Those are the kinds of things we are doing. There are some simple then protections that one can take that we have put into effect or are in the process of putting into effect without our own agency, for example, one should be very wary of what we call software that you get off the public fora, bulletin boards and that kind of thing, because you may be getting everything that you think you are getting plus something.

We restrict people in our own agency from bringing in programs from home because that may be on a disk that was in their own PC that happened to be on a network and could have been infected. We are advocates of a technique called simple check summing, and what that is is one can write at the end of a program information that tells you how many lines of code actually were on that program and one can sort of wrap the product electronically as one might wrap the product in a cellophane thing. Before using that, one could go back and say is this program the length it was when I bought it.

The bottom line is there are some simple precautions that one can take. We are advocates of not sharing too many programs and thus we would be advocates of safe computing.

Some of the problems are simple. A topic for further research are some of the more complicated problems in large operating systems. That is where we are at this point.

Mr. MCCURDY. It is amazing how medical terms are starting to pervade this area, too.

The gentleman from Maryland is well known to you all at the Center, that is within his congressional district. He has taken a great interest in this area and certainly has provided leadership in that and I recognize the gentleman from Maryland.

Mr. MCMILLEN. Thank you, Mr. Chairman. We were just recalling about a year or so ago our visit to the Center. I welcome you to the Hill and look forward to working with you in the future to ensure the implementation of this Act.

I had some questions that I would like to throw out to either of you. Certain of these questions were directed at OMB but I would also like your opinion.

From your standpoint, how would you characterize the working relationship between NIST and yourselves?

Mr. GALLAGHER. From a personal standpoint in my relationship with Jim Burrows and from an organizational standpoint, my people and people in other parts of Dr. Hearn's organization, I believe it has been thorough, enthusiastic and forthcoming. I am really very pleased in what we have done and what we are able to do together.

Of course, you will be able to get a sample of that when you do the keynote address at the next national conference and the Admiral has ticked off and Dr. Hearn has ticked off a number of things that we are cooperating on. It is not just the pro forma thing. I believe we are really working together.

Admiral STUDEMAN. Being new to the agency, I have an opportunity to measure, if you will, objectively in my own view of the level of enthusiasm in the agency, having just recently visited the Center within the last three weeks myself, and I can say quite honestly that the first element of their discussion was to basically show the responsibility they have towards, if you will, assisting with this part of the law as well as making their relationship go well with NIST.

Mr. MCMILLEN. From your standpoint, what is the status of the Memorandum of Understanding with NIST?

Admiral STUDEMAN. We are continuing to work, as I said before, we have a few issues to iron out and I'm optimistic that we will be able to iron those out.

Mr. MCMILLEN. Can you elaborate on the cryptology problems?

Admiral STUDEMAN. Let me say, I think it is unfair to fall back directly on only the cryptology issue because when you take a look at the issues related to computer security and you are dealing with the larger issue of computers which include interconnects, communications, kinds of issues, there are a whole range of issues with regard to ensuring that security mechanisms are entered into the end to end aspects of the activity.

I think it is fair to say that we need to ensure that we have a fair division of effort in terms of who will play on what part of the field relative to all those mechanisms that are involved in those security enhancement activities.

Mr. MCMILLEN. The question I have is, is the National Computer Security Center at NSA providing technical assistance to NIST in its role to develop security standards for civil application needs?

Mr. GALLAGHER. I believe we are, some manifestations of that are that we started about two and a half years ago a study that we called the secure data network study, Dr. Dennis Branstad of NIST was a full and participating member of that. The final outcome or the interim outcome has been publications that we believe are appropriate for inclusion in the OSI and GOSIP models that will allow us to do interconnects.

We have delivered as we promised on the 15th of August two of the papers which were important for a workshop that came up later in August. The other five are under review.

We believe this is a manifestation of what we think is useful. Our orange book or our Trusted Network Interpretation, our red book, and our soon to be published trusted database interpretations, we believe are all applicable in some manner across the board regardless of community because of the technology that we are talking about is apropos across the board, regardless of whether one is interested in merely confidentiality or exclusively integrity or authentication or reliability.

We think our work and we think those metrics that we create will be useful in the trusted technology, no matter what its applica-

tion, and we are sharing that with NIST for their decision as to how appropriate it is.

Mr. MCMILLEN. The last question is with regard to the National Computer Security Center. Has there been discussion to consolidate that with NIST or move it? What is the status of that? Has any consideration been given to that?

Mr. GALLAGHER. I think I'd like to defer to my bosses.

Mr. MCMILLEN. Obviously I have a parochial interest in that. I'd like to hear if there has been any discussion from either side on that matter.

Dr. HEARN. There has been no discussion.

Mr. MCMILLEN. Thank you, Mr. Chairman.

Mr. GLICKMAN [presiding]. Thank you. I apologize for coming late. Admiral, it is a pleasure to welcome you and I know we will be in contact with you many times in the months to come. As you know, along with Congressman Brooks, I was the author of this law. It does look to me like agencies of the Federal Government are taking it seriously, because the threat is serious. You all have historical experience. This law was to try to make some reason out of the way computer security functions are implemented in the Government and outside the Government as well.

I know there has been tension historically between the NSA and then the National Bureau of Standards, now the National Institute of Standards and Technology, on how to deal with these problems.

The law was in a sense a way to try if nothing else to get you folks together to allocate the functions.

From a general point of view, I wonder if you could talk about your relationships with the National Institute of Standards and Technology in connection with the implementation of this Act. Are you talking with each other? What problems are there that haven't been solved, what things have you worked out?

Admiral STUDEMAN. From my point of view and I can have the other two elaborate who know far more about it, but my sense is that they are in fact talking. Again, I think the issues that need to be resolved are issues, as in my opening statement, evolve around making sure that we have the efficiencies and economies in terms of what is done in the Federal Government in pursuit of the intent of the law, and we believe obviously that NSA can bring a great deal to that.

What we are trying to do now and I think it was captured in last year's speech in fact by Mr. McCurdy which I read excerpts from in my opening statement, which had to do with the issue of turf. In other words, who will do what, making again maximum use of expertise. That is where the issues are now focusing I think and I'm optimistic that we can reach closure on those issues as to who will do what.

Mr. GLICKMAN. Mr. Hearn?

Dr. HEARN. My perspective goes back to August 1st, because that's when I assumed my present position. But since that time, one of the first things I did was to go out to the NIST Headquarters and meet Mr. Kammer for the first time and a couple of his staff and try to get a common view on the history and where we were going in the future. And since then, we have met two other times and because, as I said in my opening remarks, the nature of

the Act will be a continuing relationship between NSA and NIST and those discussions and those meetings will have to continue to support that in a positive way.

Mr. GLICKMAN. Now I know that there have been some discussions on the issue of cryptological standards. I'm not going to get into specifics here. However, I am aware that there are still some problems between you and NIST as to developing a timetable of working some of these issues out and the nature of the classification involved in these standards. I'm concerned that we may have a problem here that may never get worked out and I want to know if you would comment on whether you've got a timetable in mind and whether you're going to reach some sort of decision reasonably soon.

Admiral STUDEMAN. From my own personal point of view, it's important that we reach a decision in the near term, and by the near term I mean not more than through the next quarter. It's relevant to any new documentation of NSDD, the specific issue of the memorandum of agreement so that we can get on with this process. And it's important that it be done before all of the, if you will, the Federal Government agencies come in with their program listings so that we can then decide how this is—the responsibilities are to be divided out.

So there's a near term requirement to, if you will, solve all of these issues.

Mr. GLICKMAN. Well, that's fine, but the question is how does it look right now? Does it look like you're going to reach some sort of—I mean, the information I hear quite candidly is that we may be approaching some sort of an impasse or deadlock between you all and NIST as to how you're going to deal with the cryptological standards and the classification issues and these kinds of things. This is not an abstract problem because obviously it relates to protection, real protection of computer information in civilian computers and both in the government and the private sector.

And I want to see it worked out and if necessary, I think that maybe we'll have to call you all in, in some sort of private meeting and sit down and talk about it.

Admiral STUDEMAN. We are proposing that in order to ensure that there is a full awareness of this and to allow us to discuss the issues and the strategies that we think are important to reaching closure on this subject, that they be discussed in another forum.

Mr. GLICKMAN. Yeah. I'm not going to do it now. But I do want to see that—you may need the impetus of the Legislative Branch to get you all together to talk about it a little bit.

Dr. HEARN. I wouldn't describe where we are presently as an impasse. I think that Mr. Kammer and I and our staffs have established a decent basis for further discussion and resolution of very tough issues.

Mr. GLICKMAN. Why don't we do this. As you know, Mr. McCurdy, of course, was involved in this as a member of the Intelligence Committee. I'm a member of the Intelligence Committee as well. And I don't want to do anything that breaches any confidentiality or classification problems either.

But I think it would be useful if, at some point in the future, we try to get together with you all and maybe with NIST people as well to talk about it.

Admiral STUDEMAN. We would very much encourage that.

Mr. GLICKMAN. Just finally, I don't know if Mr. McMillen had raised this. The whole computer virus issue, was this discussed earlier on? Are you currently doing a research on the issue of the virus situation?

Admiral STUDEMAN. I believe as you were coming in the room, Mr. Gallagher was just finishing up going through a litany of activities that his center, in fact, has been engaged in with regard to dealing with the issue of viruses.

Mr. GLICKMAN. Is this an unanticipated phenomenon, the issue of the virus or the issue of screwing up the software in some way so it just infects the whole system?

Mr. GALLAGHER. No, sir, it's not. A virus really is what we would call a subset of the larger class of problems called malicious code, which are things like Trojan Horses and things like that that can be done. So they have been well known and have studied—have been studied as an epidemic issue for some time. As I mentioned in my remarks, we had been doing that. We heated up the intensity of our pursuit of this and the creation of a taxonomy of viruses so that we can begin to deal with them as sets, and also deal with the remedies for them as they fit into sets, about eight or nine months ago.

Mr. GLICKMAN. Who came up with the terminology of virus, may I ask? It's kind of an anthropomorphic term as it relates to pieces of software and hardware. It's kind of——

Admiral STUDEMAN. We almost had reached the point where we started to talk in terms of Computer Center prophylactic kinds of responses.

Mr. GLICKMAN. Well, this isn't as serious as the AIDS problem, but now you're beginning to relate the two together.

Mr. GALLAGHER. I don't know the answer, but perhaps when Jim Burrows is here, he might know the answer to who coined the term.

Mr. GLICKMAN. Does anybody else have any questions that haven't been asked?

[No response.]

Mr. GLICKMAN. Thank you all very much, and we will try to set up a meeting with you, if possible, to talk about these issues further.

Next, we have Mr. Raymond Kammer, Deputy Director of the National Institute of Standards and Technology, accompanied by Mr. James Burrows, Director of the National Computer and Telecommunications Laboratory. Thank you very much. Glad to see you again and you may proceed as you deem appropriate. Your entire statements will appear in the record, so if you want to try to accelerate it for the purpose of questions later, we'd appreciate it.

STATEMENT OF RAYMOND G. KAMMER, DEPUTY DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, ACCOMPANIED BY JAMES BURROWS, DIRECTOR, NATIONAL COMPUTER AND TELECOMMUNICATIONS LABORATORY

Mr. KAMMER. As you all know, in early January, the Computer Security Act became law and I'll discuss our progress since then in five areas; training, review of computer security plans, establishment of the advisory board, our cooperative industry-government activities, and our technical activities.

I'll also talk a bit about our future plans and our collaboration with NSA. I've also addressed the specific questions that were posed in the invitation to testify in my longer testimony, and I won't do it here.

We've been working very closely with OPM to develop computer security training regulations for the U.S. Government. The regulation was issued in July. Other security training guides are planned before the end of this calendar year. On July 8th, we had a meeting with over 700 Federal participants in a one-day forum that was devoted to explaining the provisions of the Act itself and the requirements to the agencies.

We planned another two-day workshop this October and the topics there will both be training and preparation of the security plan. This will be our opportunity to try and help the agencies with unanticipated problems, and the instructions for the plan, and clarifications and the like. The computer security plan's guidance was provided in a bulletin that was devised by OMB, NSA, and us, Bulletin No. 88–16.

And that is out and the requirements are on the agencies now. We're discussing with NSA how we're going to handle the review of the plans when they're submitted in January. Our intent is to have the review be a co-review, simultaneous review of a cooperative team among NSA and NIST employees.

The Computer Systems Security and Privacy Advisory Board charter has been approved by the Department of Commerce. We have made selections and the backgrounds of the individuals who have been selected are being reviewed right now, which is always the case under our Public Advisory Board practice. It's reasonable to expect all the reviews to be done by the end of October.

With respect to cooperative industry-government activities, we've convened a Computer and Telecommunications Security Council which is composed of about 30 public and private sector experts. They held their first meeting last spring in April. The intent of this Council is to improve the state-of-the-art and practices of computer and telecommunications security.

Their assignment right now, if you will, is to identify security issues that are important to this community and recommend methods for addressing these issues. The Council has established a number of working groups appropriate to the issue and they just held their second meeting at the start of this week, and out of that we expect to be able to distill a plan, if you will, for reactions.

I've summarized our technical activities in 1988 in my testimony at some length, and I won't go through all of those. I would like to mention in particular one item because it also illustrates the level

of cooperation between NSA and NIST, namely the establishment of a risk management laboratory which has been done with NSA. It's located at NBS, but staffed by both agencies—at NIST, sorry, but staffed by both agencies.

And the purpose of this risk management laboratory is to both conduct research and provide advice to Federal agencies on how they can better make their risk management decisions, which is, of course, key to achieving a measure of computer security. Again, in 1988, I've summarized a series of milestones that we hope to achieve. A critical influence on this will be the budget decisions that are made.

When testifying on the formulation of this Act, I had indicated that a total program of about $6 million would be required from our point of view. We currently have a program of about a million and a quarter million, half. OMB, in the fiscal year 1989 budget, approved the submission of an increase of $5 million, which would have put us to the level intended.

Our mark is a matter of dispute between the House and Senate at the moment, and will be somewhere between zero increase and $5 million. What the result is, I'll know better what we'll be doing in fiscal year 1989 when I know our budget.

With respect to collaboration with NSA, we've been discussing our mutual roles and we've been working on a plan, if you will, for working together. Working with the NSA staff, we've written a letter which we've now sent to NSA, asking them to indicate the level of participation that they're willing to have in a number of program areas associated with developing computer security tools and standards and guidelines. And they're now considering this and will be coming back with a response, which we know will be positive. It's simply the details of the response that we're working on.

As Dr. Hearn indicated, he and I and our staffs have been meeting regularly recently, and I share his sense of optimism that it is going to be possible to resolve the issues. Not easy, but possible. There are some intellectually difficult issues and I would join with the NSA management in agreeing that a separate briefing and discussion would probably be a very useful thing.

The issues may not have conceptual solutions that will solve every case. We may have to work it through issue-by-issue to get to a satisfactory resolution. But I sense on NSA's part the willingness and the resolve to do that and we have it as well. Thank you.

[The prepared statement of Mr. Kammer follows:]

U.S. DEPARTMENT OF COMMERCE
STATEMENT OF RAY KAMMER, DEPUTY DIRECTOR
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
BEFORE THE SUBCOMMITTEE ON
TRANSPORTATION, AVIATION, AND MATERIALS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
SEPTEMBER 22, 1988

Mr. Chairman and Members of the Subcommittee:

I am here to testify on the progress NIST has made on implementing the "Computer Security Act of 1987." I am accompanied by Jim Burrows, Director, National Computer and Telecommunications Laboratory (formerly the Institute for Computer Sciences and Technology.)

In early January, the Computer Security Act became law. I will discuss our progress in meeting the assignments in five areas:

- o Training
- o Review of Computer Security Plans
- o Establishment of the Advisory Board
- o Cooperative Industry/Government Activities
- o Technical Activities

I will also talk about our future plans, collaboration with NSA and address questions you posed when you invited us to these hearings.

Requirements for Computer Security Training

We have been working closely with the Office of Personnel Management to develop a regulation for the U.S Government. The regulation was issued on July 13, 1988, as 5 CFR Part 930. A draft training guide developed by NIST has been distributed. Other security training guides to be issued by the end of 1988, will meet the needs of computer users, senior executives and managers, and computer system managers. These will assist agencies in meeting their security training obligations required by the Act.

On July 8, over 700 Federal participants attended a one day workshop cosponsored by NIST, NSA, and OPM devoted to explaining provisions of the Act. Another two day workshop is planned in October to assist agencies in meeting requirements for training and in developing security plans to be submitted in January.

Development and Submission of Computer Security Plans

We worked with NSA and OMB in the development of Bulletin No. 88-16, which provides guidance for the preparation and submission of security plans. We are already developing plans with NSA on our joint review of the agency plans in January of next year.

The Computer System Security and Privacy Advisory Board

A charter has been approved by the Department of Commerce for the Computer System Security and Privacy Advisory Board established

under the legislation. Nominations of many distinguished and well qualified candidates have been received. The selections have been made, and those selected are currently being cleared under the Department's procedures for public advisory boards, prior to their being announced.

Cooperative Industry/Government Activities

The Computer and Telecommunications Security Council composed of about 30 experts from the public and private sectors held its first meeting in April. The Council was established by NIST to improve the state-of-the-art and practices of computer and telecommunications security.

One objective of the Council is to identify security issues of significant importance to the computer and telecommunications community, and to recommend methods for addressing these issues. The Council established several working groups to investigate topics including: network security, data integrity, physical security, audit methods, and future technology. A second meeting of the Council held on September 19 and 20, further refined issues and planned follow-on actions.

Technical Activities in Fiscal Year 1988

During the current fiscal year, we continued our technical program based on the foundation of technical, management, physical, and administrative security standards and guidelines

that have been developed and issued since the mid-1970s. These standards and guidelines were developed and tested in laboratory-based research facilities, often in collaboration with other government and industry organizations. Many of the existing standards and guidelines are valid and appropriate for today's technology. However, as technology changes, these standards and guidelines must be updated, and new laboratory initiatives started. Because of our focus on completing the work needed to meet schedules established by the legislation, we were not able to carry out all of the major new studies needed to update old standards or to develop new ones. Some of the technical activities engaged in during Fiscal 1988 are described below.

NIST established a Risk Management Laboratory in collaboration with the National Security Agency. The laboratory will be used for research to improve tools, techniques, and guidance needed for risk management, and as a focal point for assisting Federal agencies in the selection and use of commercial risk management software. Good risk management techniques are essential for carrying out the Computer Security Act's emphasis on "cost effective" security and privacy. The risk management process enables computer users to analyze their information assets, threats, and vulnerabilities, to determine the measure of risk and to select cost effective safeguards for reducing the risks. NIST contributed to international efforts to improve risk management methods through participation in the First International Workshop on Computer Security Risk Management.

A guide to auditing the system development life cycle of an automated information was issued as Special Publication 500-153, "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach." Developed in cooperation with the President's Council on Integrity and Efficiency (PCIE), the guide provides assistance to auditors, security reviewers, and quality assurance personnel in auditing a system for controls and security.

Another publication issued this year describes the validation system we developed to test message authentication devices for conformance to data authentication standards. Special Publication 500-156, "Message Authentication Code (MAC) Validation System: Requirements and Procedures", draws on work that was done for the Department of Treasury. The Message Authentication Code uses data encryption techniques to protect against accidental and intentional modification of data that is transmitted between computer systems.

Another publication completed this year is Special Publication 500-157, "Smart Card Technology: New Methods for Computer Access Control." This research report describes the essential characteristics of smart cards and how these cards may be used to authenticate the users of modern computer networks.

We continued to contribute along with NSA and Treasury to the development of voluntary industry standards for protecting

financial data transmitted through networks. As in the past, we have been active participants in the work of banking industry's standards committees.

The recent approval of Federal Information Processing Standard 151 for POSIX (Portable Operating System Interface for Computer Environments) points up the pervasive requirements for security features as new standards are developed. To help extend security controls to POSIX systems, we have taken a leadership role in the voluntary standards committee (Institute of Electrical and Electronics Engineers P1003.6) that is developing POSIX security standards.

Planned Activities in Fiscal Year 1989

During the next fiscal year, we expect to build on the activities that we have started this year to improve the cost-effective security of sensitive information in Federal computer systems. Among the planned activities are the following:

We will continue to develop training guidance and technical materials to be used for computer and telecommunications security training and awareness-building. Because of the large number of Federal employees whose awareness must be raised, we will suggest various, alternative methods for delivering the training, including videotapes, computer-based instruction, employee workbooks, posters and brochures.

Along with NSA, we will review plans submitted by the agencies and provide advice and comments on those plans.

We will assist the Computer Systems Security and Privacy Advisory Board in carrying out the duties established in the legislation.

Risk management methods, standards and guidelines will be developed to enable Federal agencies to consider and adopt cost effective protective measures for their sensitive information.

Technology transfer with Federal agencies and the private sector will be strengthened. We must work together to achieve common solutions to common problems in security planning, risk management, identification of security requirements, and application of standards and guidelines.

New working relations will be initiated with government and industry to improve the state-of-the-art and practice in computer and telecommunications systems security, and to achieve widespread application of methods that are suitable for both government and industry.

Collaboration with NSA

The Act calls for NIST to coordinate closely with other agencies and offices to assure maximum use of all existing and planned programs, materials, studies and reports related to computer systems security and privacy. It also calls for assurance that

standards which are developed are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems authorized under criteria established by Executive order or an Act of Congress to be kept secret for national defense or foreign policy.

We have been discussing with NSA our mutual roles with respect to the legislation. NIST and NSA are working on a wide variety of security initiatives. NIST recently made formal requests for assistance to NSA in a number of computer security areas. These requests have been made to the Director of the National Computer Security Center. The requested assistance includes: the development of technical guidelines upon which security standards may be built; the results of NSA-sponsored research; guest workers at NIST to perform specific projects; and evaluation of proposed security standards.

The following sections, respond to your questions about civilian versions of certain computer and network security guidance provided by NSA.

Secure Data Network System (SDNS)

Question: What plans does NIST have for developing a civilian version of the Secure Data Network System (SDNS) including NIST public key and key management standards and using the NIST Data Encryption Standard as the Type III encryption standard for SDNS?

Answer: A goal of the NIST security program is to develop a set of standards that may be implemented in off-the-shelf computer systems and useful in a wide range of security applications.

NIST recognizes that any security system should be designed so that new security requirements may be satisfied with minimum changes to the system. If a security architecture, including security services, protocols and mechanisms, is designed in a modular fashion, the majority of the modules will remained unchanged even if components, such as a cryptographic algorithm, are replaced.

NSA initiated development of the Secure Data Network System in 1985. SDNS was based on the Open Systems Interconnection (OSI) computer network model and was to embody NSA developed cryptography in two families of products.

Seven documents have been developed as the result of the SDNS project that specify security services and protocols for user data as well as supportive services, including key management and access control. Two of these seven documents were released by NSA thus far for use by NIST in its development activities and by other organizations seeking to adopt SDNS technology.

NIST is considering reviewing and adopting the SDNS security protocols as Federal Information Processing Standards as they become available for public review.

TCSEC Evaluation Criteria (Orange Book)

Question: What plans does NIST have for developing a civilian version of the Trusted Computer Security Evaluation Criteria (TCSEC)?

Answer: NIST plans to work with the NCSC in augmenting the TCSEC with requirements for integrity and availability. NIST will not initiate development of a FIPS guideline or standard on trusted systems until agency requirements for integrity and availability have been addressed. These plans are based on the following rationale.

NIST believes that all agencies processing unclassified but sensitive information in computer systems which are accessed by more than one user, when those users do not have the same authorization to use all of the information processed or maintained on the computer system, agencies should conduct a risk assessment. Based upon its results, should consider using operating systems providing Trusted Computer System Evaluation Criteria (TCSEC) C2 level of protection (i.e. Controlled Access Protection) to enhance user access controls. If available and cost effective, operating systems that have been evaluated as C2 by the NCSC should be used. If there are no such evaluated products available for use, then agencies can select operating systems that best meet the criteria of C2

until such products become available.

Agencies that process unclassified sensitive information in shared computer systems that need, as determined by a risk assessment procedure, a system-enforced (i.e., software/hardware) mandatory access control policy, should consider using operating systems with TCSEC Division B protection. If available and cost effective, operating systems that have been evaluated as B1 or B2 by the NCSC should be used.

Historically, NIST does not evaluate or endorse products of any kind. However, as part of developing a standard, NIST may develop conformance tests which can be used by NIST, product developers, end users, and approved testing organizations to test the conformance of a product to the standard.

Trusted Network Interpretation (TNI)

Question: What plans does NIST have for developing a civilian version of the Trusted Network Interpretation (TNI) including assuring that SDNS capabilities are compatible with and directly related to the TNI?

Answer: The National Computer Security Center issued the "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" in July, 1987. The TNI (often called the Red Book) extends the scope of the TCSEC (often called the Orange Book) to computer networks.

Since TNI is still a draft, we cannot comment on the development of a civilian version of the document. NIST is interested in security in distributed systems for unclassified applications and will use the TNI and its successor documents as inputs when this work is initiated.

Trusted Data Base Interpretation (TDBI)

Question: What plans does NIST have for developing a civilian version of the forthcoming Trusted Database Interpretation of the TCSEC?

Answer: The Trusted Data Base Interpretation is not yet a draft; therefore it is premature to comment. However, NIST is interested in conducting research in distributed database security and integrity and providing guidance identifying issues and risks and recommending management and technical solutions for securing unclassified but sensitive data base systems.

Mr. GLICKMAN. Okay. It's a good time to stop. We have a vote right now. We'll be back in about 10 or 15 minutes, and we'll come back and, Mr. Burrows, did you have comments, too, or we'll just go to questions then.

[Brief recess.]

Mr. GLICKMAN. Thank you. sorry about the votes. We'll try to move this as quickly as possible. I would ask—you mentioned this a little bit before, but I just want to get this on the record, Mr. Kammer and Mr. Burrows, to characterize where you are right now in terms of reaching an agreement on the cryptology issue and working this out.

Mr. KAMMER. We have had extensive discussions of it. I think we've both come to understand the operational needs and the mission needs of the other, if you will. Some of the requirements for both sides are going to require a little bit of give by the other side. We have come to recognize that.

My belief is that we will be able to find a resolution. As I suggested to you a little bit earlier, I'm not sure it's going to be a conceptual resolution, if you will—three or four sentences that easily explain it. It may be that on an item-by-item basis in some of the areas, we're just going to have to go through and think of a practical solution for that problem.

I am optimistic about our ability to do that. Jim, perhaps, ought to comment too.

Mr. GLICKMAN. As you go back and read the law, and I say this for both your benefit as well as the NSA's benefit, and this, of course, comes out of Dr. Hearn's testimony; the law requires you all to draw upon the technical assistance and work products of NSA as deemed appropriate for use in protecting sensitive government data—unclassified sensitive government data.

Now, this relates to cryptological work as well as it relates to non-cryptological work. However, I do believe it was the intent of Congress that you would maintain your role as essentially the lead agency in this regard. I am first and foremost interested in protecting data. I am less interested in who does it, except to the extent that we want to keep civilian agency monitoring control over what's going on here.

As we work on this problem, I think you have to go back to the statute and figure out what Congress had intended in this regard. You know, there was a clear intent about general direction of where we wanted to go. At the same time, build on NSA's historical knowledge. I know this is difficult to do, because I know that historically, there are forces at NSA who frankly did not want to relinquish any control whatsoever of any of these issues.

We did it; we developed it; we built it, and the whole sensitive issue was related so closely to the classification issue, that there was not the desire to break away from that historical pattern. This bill said we want to do things slightly differently in the future. I hope that we can work those things out. At the same time, I recognize that it is not my desire to breach classification information, whether it be for the use of the Soviets or for the use of criminal elements in this society either.

We just need to try to work it out, because it is going to become a more serious problem all the time.

For the record, how do you assess the progress of federal agencies in developing computer security plans as required by the law?

Mr. KAMMER. I'm going to ask Mr. Burrows to comment on that.

Mr. GLICKMAN. All right, Mr. Burrows.

Mr. BURROWS. Well, of course, prior to the law, many of the agencies did have plans. Some of them had very credible plans, but I think that those who did not have formal plans are complying. The detail to which the plans have to go in terms of what they cover means that there are a lot of plans that have to be prepared. That means we're going to get a lot of data to look at in January.

I think we're moving ahead and we have a correction meeting in October when we'll be able to answer questions and give examples of people who have already prepared plans and talk about difficulties they are having so we can help them get to the January 8th deadline.

Mr. GLICKMAN. Do you sense that the agencies are calling upon your expertise to do this?

Mr. BURROWS. I think they do call us, but I think they pretty much know what's needed. It's the volume of what's needed that's, I think, catching them up.

Mr. GLICKMAN. The volume of what? What are you talking about?

Mr. BURROWS. Well, the number of plans they have to prepare, since it's by system, not by agency. It's not a general plan we've asked for; it's a very specific plan.

Mr. GLICKMAN. There is a concern that you all have not developed—that is, the National Institutes of Standards and Technology—have not developed or not issued any security standards for sensitive information systems under development. What approach do you plan to use in developing uniform security standards and guidelines for the civil agencies for sensitive systems under development and in operation?

Mr. BURROWS. Well, I can tell you what I think we'll be doing. The process of developing a computer telecommunications information system is a very detailed and laborious process in which lots of things have to be kept in mind. We have been preparing for the last 15 years, management guides on things that should be thought about and processes which should be executed in order to plan and bring into being an information system.

Security is just another manifestation of good management—much of security is. Some security is very special, but a lot of it is just good engineering. I think we've been trying to get people to use those techniques for 12–15 years. That means a change in the way people work; a change in their management, a change in the expectation of various people as to the steps in which things get done, and a change in the way they test things.

Those kinds of documents have come out. They haven't been labeled security, but they have come out.

Mr. GLICKMAN. Do you plan a civil version of the NSA's orange book?

Mr. BURROWS. We plan an augmentation of the orange book which we hope will cover also the areas of availability and integrity. We're working with them to get on with that job.

Mr. GLICKMAN. Specifically, what's your schedule for developing the security standards and guidelines?

Mr. BURROWS. I guess schedules depend both upon availability and due to the way in which we work, which is different from NSA from my point of view; we work in a very open environment where the people who are going to be impacted by the guideline or the standard take an active part in the development of the guidelines and standards.

When it's over, it's not a problem of selling it to somebody. They already know what it is, and they can go ahead and do it. That, if it really requires something, for example, like the orange book requires that manufacturers change the equipment and the suite of software which they send to you; that means turning it into a national standard. That's a very laborious process and may take 3-5 years.

Mr. GLICKMAN. There is an advisory board under the statute, the Computer Systems Security and Privacy Advisory Board within the Department of Commerce. I understand there have been some delays. When will the Board schedule its first meeting?

Mr. BURROWS. I think everything will be in place according to the advisory rules for advisory committees, by the end of October, and we should have our first meeting in November. One of the problems is going to be to get those people scheduled to a common date. They come from industry and various parts—they probably should have at least two months' warning about the meeting in order that they can schedule their time.

Mr. GLICKMAN. I'm skipping around a bit, but there is such a variety of things. The Office of Personnel Management has training regulations. Have you issued any comments on those training regulations?

Mr. BURROWS. We helped them produce those.

Mr. GLICKMAN. How do you feel about them?

Mr. BURROWS. I think for the level of detail which was required at that time, they're what we needed. I think as time goes on, we'll discover what additional training activities are available and what things we want to get across. They'll probably be augmented at that time.

Mr. GLICKMAN. Let me finalize with the question I asked NSA at the end about this computer virus issue. Are you doing research into this issue?

Mr. BURROWS. We've known that NSA has been doing extensive research and traveling around the country and talking to people, and we have not done that. We have had access to what they're doing. There was a question earlier which was, where did the term virus come from? It turns out, back in the 70's, there was a lot of interest in self-reproducing programs.

Then there got to be an interest in attaching self-reproducing programs to other programs so that you could move them around. Then there got to be, well, while we're moving around, let's have it do something more than self-reproduce; let's have it do something to the host that it's in—either blow a whistle, make a nasty word come up on the screen, or foul up the whole system.

Back in about 1978, I believe, a guy by the name of Fred Cohn who was working with ARPA at that time and the research com-

munity brought up the name virus. It was a sort of underneath the covers sort of thing for about five years. Then it sort of broke out and more people knew about it—knew about the capability. Indeed, I think about four or five years ago, at one of our conferences, we had a paper on viruses.

They do have the kind of capabilites that you think of as viruses and Fred was very innovative in picking that name.

Mr. GLICKMAN. How serious of a threat are these viruses to government computers?

Mr. BURROWS. I think it was stated that the things like viruses, bombs, and other things, can be inserted into code by your own employees if they don't like you. I think that's one of the reasons why when we have disgruntled employees or people that we are about to fire, we want to get them off the premises as fast as possible so they don't have time to do that kind of thing.

I think that's going to be the major source. I think the idea of importing them from outside, if you're wise about how you run your installation, you can avoid that.

Mr. GLICKMAN. Do you mean through, like telephone lines?

Mr. BURROWS. That's right.

Mr. GLICKMAN. Microwaves?

Mr. BURROWS. Asking to have people send you stuff which you then want to run. If you don't trust them or if you just say send me what you have, like we do in PCs when we say there are Free programs downtown, take what you want. And the answer is, take what you want, but beware, it may not be what you think it is.

I think when you're running a commercial installation for work, you try to avoid that. Your biggest problem is somebody who wants to hurt you. That's usually a disgruntled employee.

Mr. GLICKMAN. Okay. Thank you for your testimony today, and we will be back in contact with you on some of the issues that we talked about before.

Our next witness is John Lafferty, Deputy Associate Director for Training and Investigations, OPM, Office of Personnel Management.

Thank you for coming and your entire statement will appear in the record.

STATEMENT OF JOHN J. LAFFERTY, DEPUTY ASSOCIATE DIRECTOR FOR TRAINING AND INVESTIGATIONS, OFFICE OF PERSONNEL MANAGEMENT

Mr. LAFFERTY. Thank you, Mr. Chairman. I had thought that in the interest of time, perhaps I could summarize briefly.

As already mentioned, the required regulation was published in July. There is, however, considerably more to implementing the Act than just the training requirement and publishing a regulation.

We have under development in OPM a series of training materials which we will be getting out this fall. We will be distributing those materials to all of the agencies in the Executive Branch that care to use or adapt them, and in addition, that same material will be available for delivery through our own training organization at various locations where we operate around the country.

That is pretty well where we are at the moment, sir.

[The prepared statement of Mr. Lafferty follows:]

STATEMENT OF
JOHN J. LAFFERTY, DEPUTY ASSOCIATE DIRECTOR
FOR TRAINING AND INVESTIGATIONS
OFFICE OF PERSONNEL MANAGEMENT

before the

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

on

PUBLIC LAW 100-235

THE COMPUTER SECURITY ACT OF 1987

September 22, 1988

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

THANK YOU FOR INVITING ME TO PRESENT THE VIEWS OF THE OFFICE OF PERSONNEL MANAGEMENT ON THE PROGRESS OF IMPLEMENTING THE COMPUTER SECURITY ACT OF 1987. WE WELCOME THE OPPORTUNITY TO EXPLAIN OUR ACTIVITIES TO THE CONGRESS.

AS REQUIRED BY THE LAW, WE HAVE ISSUED A REGULATION WITHIN 6 MONTHS OF ENACTMENT FOR THE TRAINING OF FEDERAL EMPLOYEES IN COMPUTER SECURITY AWARENESS AND SECURITY PRACTICES. OUR REGULATION REQUIRES THAT THE HEAD OF EACH AGENCY IDENTIFY THOSE EMPLOYEES WHO WORK WITH COMPUTER SYSTEMS THAT PROCESS SENSITIVE INFORMATION AND PROVIDE THEM WITH AN AWARENESS OF THE VULNERABILITIES OF AND RISKS TO THE COMPUTER SYSTEMS AND AN ABILITY TO APPLY THEIR AGENCY'S COMPUTER SECURITY PRACTICES AND PROCEDURES. THE REGULATION SPECIFIES A SET OF TOPICS IN COMPUTER SECURITY PRACTICES AND PROCEDURES FOR WHICH EACH AGENCY SHALL PROVIDE TRAINING AS APPROPRIATE. THE REGULATION REQUIRES THAT TRAINING SHALL OCCUR WHENEVER THERE IS A SIGNIFICANT CHANGE IN THE AGENCY'S INFORMATION SECURITY ENVIRONMENT OR PROCEDURES. FINALLY, THE AGENCY MUST PROVIDE REFRESHER TRAINING AS FREQUENTLY AS DETERMINED NECESSARY BY THE AGENCY BASED ON THE SENSITIVITY OF THE INFORMATION. WE HAVE SUBMITTED A COPY OF THE REGULATION TO THE SUBCOMMITTEE FOR THE RECORD.

THE OFFICE OF PERSONNEL MANAGEMENT HAS TAKEN A REGULATORY APPROACH THAT STRESSES THE ACCOMPLISHMENT OF MANAGEMENT OBJECTIVES RATHER THAN DETAILED PROCEDURES. CONSISTENT WITH THAT APPROACH, OUR REGULATION SETS GOALS FOR AGENCIES SO THAT THEY CAN MEET THE INTENT OF THE LAW. THE WORKING ENVIRONMENTS OF AGENCIES ARE SO DIVERSE THAT A PROCEDURALLY ORIENTED REGULATION WOULD BE DISRUPTIVE TO AGENCY OPERATIONS AND WOULD NOT SUCCEED IN MEETING THE GOALS OF THE LAW. SOME AGENCIES ALREADY HAVE STRONG COMPUTER SECURITY AWARENESS PROGRAMS IN THE SENSITIVE INFORMATION AREA THAT IS THE SUBJECT OF THIS LAW. IF OPM WERE TO WRITE A VERY SPECIFIC REGULATION WE COULD NOT POSSIBLY ENCOMPASS EVERY AGENCY'S PRACTICES. THEN SOME AGENCIES WOULD HAVE TO CHANGE PROGRAMS THAT WERE FUNCTIONING WELL MERELY TO COMPLY WITH THE REGULATION, OR INVOKE THE AUTHORITY GIVEN BY SECTION 5 (a)(2) OF THE ACT TO APPROVE THEIR OWN PROGRAMS AS ALTERNATIVES.

WE ALSO BELIEVE THAT OUR APPROACH IS REASONABLE BECAUSE, DURING THE COMMENT PERIOD, WE RECEIVED ONLY ONE RESPONSE FROM AN AGENCY AND THAT WAS PROCEDURAL RATHER THAN SUBSTANTIVE.

ON JULY 8, 1988, THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY AND THE U.S. OFFICE OF PERSONNEL MANAGEMENT ISSUED DRAFT COMPUTER SECURITY TRAINING GUIDELINES TO THE FEDERAL COMMUNITY, IN RESPONSE TO REQUIREMENTS SET FORTH IN THE COMPUTER SECURITY ACT. THE COMPUTER SECURITY ACT STATES THAT, "EACH FEDERAL AGENCY SHALL PROVIDE FOR THE MANDATORY PERIODIC TRAINING IN COMPUTER SECURITY AWARENESS AND ACCEPTED COMPUTER SECURITY PRACTICE OF ALL EMPLOYEES WHO ARE INVOLVED WITH THE MANAGEMENT, USE, OR OPERATION OF EACH FEDERAL COMPUTER SYSTEM WITHIN OR UNDER THE SUPERVISION OF THE AGENCY." THE DRAFT COMPUTER SECURITY TRAINING GUIDELINES ARE CURRENTLY UNDER REVIEW BY THE AGENCIES AND OPM IS PARTICIPATING IN THE REVISION PROCESS.

IN ADDITION, OPM IS DEVELOPING COMPUTER SECURITY AWARENESS TRAINING TARGETED AT SPECIFIC AUDIENCES BASED ON THE REQUIREMENTS OF THE ACT, THE REGULATIONS, AND THE TRAINING GUIDELINES. OPM WILL PROVIDE A NUMBER OF TRAINING OPTIONS TO ASSIST FEDERAL AGENCIES IN CONDUCTING THEIR OWN TRAINING AND WILL ALSO PROVIDE TRAINING THROUGH OPM'S OWN TRAINING DELIVERY SYSTEM.

IN THE DEVELOPMENT OF THESE TRAINING MATERIALS, OPM IS PAYING PARTICULAR ATTENTION TO EXISTING TRAINING MATERIALS AND, WHERE APPROPRIATE, THEY WILL BE INCORPORATED INTO THE NEW TRAINING MATERIALS. OPM HAS ESTABLISHED AN INTERAGENCY WORK GROUP ON COMPUTER SECURITY AWARENESS TRAINING THAT IS REVIEWING AND PROVIDING REACTION TO THE APPROACH AND SUBSTANCE OF THE TRAINING MATERIALS AS THEY ARE BEING DEVELOPED.

THE FOLLOWING TRAINING MATERIALS ARE UNDER DEVELOPMENT AND WILL BE AVAILABLE TO FEDERAL AGENCIES THIS FALL:

A COMPUTER SECURITY AWARENESS VIDEOTAPE SPECIFICALLY HIGHLIGHTING THE REQUIREMENTS OF THE ACT AND THE COMPUTER SECURITY TRAINING GUIDELINES.

A COMPUTER SECURITY AWARENESS JOB PERFORMANCE AID WHICH WILL BE A COMPUTER SECURITY CHECKLIST CROSS-INDEXED TO SPECIFIC REFERENCES OR RESOURCES.

AN EXECUTIVE BRIEFING FOR SENIOR MANAGERS THAT WILL INCLUDE BRIEFING NOTES AND PARTICIPANT MATERIALS.

A ONE-DAY COMPUTER SECURITY AWARENESS COURSE THAT INCLUDES LESSON OUTLINES, DISCUSSION QUESTIONS, PROBLEMS, CASE STUDIES, GROUP EXERCISES, TRANSPARENCIES, INSTRUCTOR HANDBOOK, AND PARTICIPANT MATERIALS.

INDEPENDENT STUDY MATERIALS, FOR USE AS AN ALTERNATIVE TO CLASSROOM TRAINING.

LASTLY, WE EXPECT TO PRODUCE BY DECEMBER, COMPUTER-BASED INSTRUCTION EXERCISES WITH SUPPLEMENTAL PRINT INFORMATION.

CONTAINING A SERIES OF INTERACTIVE SITUATIONS AND PROBLEMS POSED IN SIMULATION FORMAT.

BESIDES ISSUING THE TRAINING REGULATIONS WE HAVE BEEN ACTIVELY INVOLVED IN DISSEMINATING INFORMATION IN ORDER TO INCREASE THE LEVEL OF RECOGNITION OF THE IMPORTANCE OF COMPUTER SECURITY TRAINING AND AWARENESS.

RECOGNIZING THE DIVERSITY OF MANAGERS WHO MAY BE IN CHARGE OF IMPLEMENTING THE ACT WITHIN THE AGENCIES, WE HAVE ATTEMPTED TO REACH A BROAD RANGE OF FEDERAL MANAGERS WHO ARE DIRECTLY RESPONSIBLE FOR IMPLEMENTATION. THE FUNCTIONAL AREAS THAT WE INITIALLY SEE AS KEY ARE THE INFORMATION RESOURCES MANAGEMENT OFFICIALS, THE COMPUTER SECURITY OFFICERS, THE TRAINING OFFICERS AND THE ADP MANAGERS.

IN ORDER TO PROVIDE INFORMATION REGARDING AWARENESS TRAINING AND PRACTICES, WE HAVE SPOKEN TO GROUPS SUCH AS THE INTER-AGENCY INFORMATION RESOURCES MANAGERS, THE INTERAGENCY GROUP ON TRAINING AND DEVELOPMENT AND VARIOUS FORUMS FOR COMPUTER SECURITY OFFICERS, ADP MANAGERS, AND AN AD HOC GROUP OF COMPUTER SECURITY TRAINERS.

WE HAVE ALSO GIVEN PRESENTATIONS TO A VARIETY OF AGENCIES' INTERNAL WORKSHOPS ON THE IMPLEMENTATION OF THE ACT. WE HAVE ALSO BEGUN TO PROVIDE BRIEFINGS AT MEETINGS OF FEDERAL EXECUTIVE BOARDS THROUGHOUT THE COUNTRY. WE WILL CONTINUE TO BE ACTIVELY ENGAGED IN BRIEFINGS AND WORKSHOPS THROUGHOUT THE FALL AND WINTER.

THANK YOU. I WOULD BE PLEASED TO ANSWER ANY QUESTIONS THE COMMITTEE MAY HAVE.

federal register

Wednesday
July 13, 1988

Part II

Office of Personnel Management

5 CFR Part 930
Training Requirement for the Computer Security Act; Interim Regulation

OFFICE OF PERSONNEL MANAGEMENT

5 CFR Part 930

Training Requirement for the Computer Security Act

AGENCY: Office of Personnel Management.

ACTION: Interim regulation.

SUMMARY: This regulation implements Pub. L. 100–235, the Computer Security Act of 1987, which requires training for all employees responsible for the management and use of Federal computer systems that process sensitive information. Under the regulation agencies will be responsible for identifying the employees to be trained and providing appropriate training.

DATES: Interim rule effective July 13, 1988. Submit written comments on or before September 12, 1988.

ADDRESSES: Send written comments to Mr. Harold Segal, Chief, Policy and Oversight Branch, Office of Training and Development, Training and Investigations, Office of Personnel Management, P.O. Box 7230, Washington, DC 20044, or deliver to 1121 Vermont Avenue NW., Room 1215, Washington, DC 20005.

FOR FURTHER INFORMATION CONTACT: Ms. Constance Guitian, Policy and Oversight Branch, (202) 632–9769.

SUPPLEMENTARY INFORMATION: Public Law 100–235, the "Computer Security Act of 1987", requires mandatory periodic training for all employees involved in the management or use of Federal computer systems that contain sensitive information. In order to accomplish this goal the law requires the National Bureau of Standards (NBS) to develop guidelines for the training of employees in security awareness and accepted security practices. The Office of Personnel Management (OPM), however, is required to issue regulations for the training within six months (July 6, 1988) of the passage of the law. The law further requires that agencies initiate training within 60 days of the issuance of the regulation. This means that agencies should start their training programs by September 8, 1988.

The preparation of these regulations required extensive coordination with NBS. Pursuant to sections 553 (b)(3) and (d)(3) of title 5 of the United States Code, I find that good cause exists to make this amendment effective in less than 30 days. The regulation is being made effective immediately in order to meet a statutory deadline. Even though we are issuing these regulations as interim effective immediately, we are inviting comments for a 60-day period. Those comments will be given consideration in the final regulations which we plan to issue within 120 days after the comment period. OPM has worked with NBS in defining areas that should be included in training activities and these are embodied in the regulation. The principal features of the regulation are:

(1) The subject matter of the training should stress awareness of the computer system's vulnerabilities and risks and be organized around each agency's computer security policies, practices and procedures;

(2) Training is a continuing process; and,

(3) Refresher training must be provided as appropriate.

The depth of coverage for each of the subjects listed in the regulation should depend on the sensitivity of the data to which the employee has access and the employee's level of responsibility and authority with respect to the information. Each agency will have to decide the appropriate level of training for its employees. The agency may include computer security awareness as a part of existing computer training, management courses and employee orientation. In addition, agencies should explore non-classroom modes of delivery of training such as computer assisted training, video tapes, workbooks, job aids and desk guides.

The Congressional Budget Office estimates that about half of all Government employees will need computer security training to make them aware of the vulnerability of sensitive information and the risks of unauthorized use. Training for most of these employees will not be technical in nature but will teach them how to safeguard the information to which they have access. Although training is of vital importance to a security program, it is only a part of a larger information management system. Agency management needs to foster a work environment where information security is seen as critical to accomplishing the agency's mission.

This regulation will be issued in Part 930 of the Code of Federal Regulations and subsequent Federal Personnel Manual guidance will be issued as an appendix to Chapter 410. The regulation may be changed when NBS issues its guidelines. The law allows the agency head the option to exempt the agency from the training requirements of the guidelines if it is determined that the agency has an alternative training program at least as effective as the one described in the guidelines.

Office of Personnel Management.

Constance Horner,

Director

Accordingly, the Office of Personnel Management adds Subpart C to Part 930 to read as follows:

Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems

Sec.

930.301 Training requirement.
930.302 Initial training.
930.303 Continuing training.
930.304 Refresher training.

Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems

Authority: 40 U.S.C. "759 note.

§ 930.301 Training requirement.

(a) The head of each agency shall identify and provide training in computer security, which emphasizes an awareness of the vulnerabilities and risks of the systems to all employees responsible for the management or use of Federal computer systems[1] that process sensitive information.[2]

(b) The objective of the training is to provide employees an awareness of the vulnerabilities and risks of the computer system. The training should also provide the knowledge and skills needed to apply an agency's computer security policies, practices, and procedures.

(c) The training shall include as appropriate agency computer security practices and procedures for:

(1) Meeting information security objectives;

(2) Responsibility and accountability;

(3) Information accessibility, handling, and storage;

(4) Physical and environmental hazard protection;

(5) System and data access controls;

(6) Emergency and disaster situations;

[1] Under the statute, the term "Federal computer system": (A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

(B) includes automatic data processing equipment as that term is defined in section 111(e)(2) of the Federal Property and Administrative Services Act of 1949.

[2] Under the statute, the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy

(7) Identification of threats and vulnerabilities; and

(8) Other security related matters.

§ 930.302 Initial training.

The head of each agency shall start the initial required training for all employees responsible for the management or use of Federal computer systems that process sensitive information within 60 days of the effective date of this regulation. The head of the agency shall provide the initial required training to all such new employees within 60 days of their appointment.

§ 930.303 Continuing training.

The head of each agency shall provide training whenever there is a significant change in the agency information security environment or procedures.

§ 930.304 Refresher training.

Computer security awareness refresher training which covers, as appropriate, the topics outlined in § 930.301 of this part shall be given as frequently as determined necessary by the agency based on the sensitivity of the information.

[FR Doc. 88-15659 Filed 7-8-88; 2:52 pm]

BILLING CODE 6315-01-M

Mr. GLICKMAN. Thank you. Have you and your agency in any way characterized the level of proficiency or deficiencies in computer awareness, computer training at any of the Federal agencies?

Mr. LAFFERTY. We have not to my knowledge in the past done anything systematic along that line, Mr. Chairman.

Mr. GLICKMAN. From your knowledge of agency plans to provide training, will most agencies use their own training capabilities, OPM courses or contracted training services from the outside?

Mr. LAFFERTY. If past experience is any guide, and I think it is in this case, most agencies will—I need to really divide agencies into two categories. As has been suggested earlier, there are some agencies as you well know which already are quite adept in this area, quite well organized. The concern is rather with the second group of agencies that have perhaps not given the matter as much attention.

Typically what will happen will be those agencies will take the material which OPM makes available, depending on how many people they need to train to meet their need, they will either take our material, use it as is, if it needs adaptation, adapt it to their particular circumstances. They may either deliver it themselves through their own training staff and using some of their own specialists on their staffs, or in cases in which they have a relatively small number of people to train, they will send them to OPM courses because it is a cost effective alternative.

Some agencies may choose, because the principal responsibility under the statute is assigned to the head of each agency, an agency may if it chooses take its own course entirely and simply open the competition, select a contractor to do the whole job. That is perfectly appropriate under the statute as well.

Mr. GLICKMAN. Are you monitoring all of this to make sure each of them are doing it and doing it effectively? Is there a system of accountability that OPM—is it OMB that is doing that?

Mr. LAFFERTY. The agency's plans, as I understand it, are expected to indicate how they are going to deal with the training component as well. The OMB channel will be the reporting channel but the information will come to us.

Mr. GLICKMAN. Now that you have had 60 days after the publication of the regulations, have agencies begun training?

Mr. LAFFERTY. Here again, I have to mention that agencies are really in two categories. Those which had existing computer security awareness programs and systems have not had to make any major modification. They are continuing to do what they have always done. Those that had very little in place do not have much in place today.

Mr. GLICKMAN. They do not? Have they started? Have you seen anything in the last 60 days?

Mr. LAFFERTY. What we have seen has been agencies that are on the short side, so to speak, have begun getting out internal instructions within their own organization saying these are the things we need to do to comply with the Act, but I cannot say that an agency that is in that category has today actually started delivering training classes.

Mr. GLICKMAN. What role does OPM have to make sure that training continues and intensifies, particularly with those agencies on the short end?

Mr. LAFFERTY. Once we have seen the materials which will come into OMB in January, we can follow up, first of all. Secondly, there are other reporting mechanisms already in existence onto which we can graft a reporting requirement, for example, an annual report of training which agencies are required to prepare in any case under the Government Employees Training Act. That is an annual submission. We can graft a reporting requirement onto that, gather status information once a year that way.

Mr. GLICKMAN. Do you intend—I guess my question is, is this a high priority at OPM? We want it to be a high priority. Is it a high priority in terms of making sure that agencies are continually prodded on their computer security training?

Mr. LAFFERTY. We will be following up, sir.

Mr. GLICKMAN. We would be interested as time goes on, on what oversight you plan to do to assure that agencies are following up. Can you provide the Committee perhaps in writing if you don't have it now, specifically what kind of oversight you intend to do to make sure that follow up occurs?

Mr. LAFFERTY. Yes, sir. I will provide that for the record.

[Information to be furnished follows:]

We share the Committee's concern that agencies comply with the training provision in the Computer Security Act. We are therefore giving oversight of agencies' computer security training a high priority. Our comprehensive oversight plan calls for the following:

1. Computer Security Training Oversight - We will work closely with GAO, NIST, and NSA to develop baseline data. We expect to have our training oversight baseline established by early Spring, 1989 and will take necessary follow-up actions at that time.

2. Computer Security Policy and Guidance - We will publish our final Computer Security Training Regulation in January, 1989 and will re-examine it in the fourth quarter, FY 1989, to determine if it needs revision. We will continue to provide NIST advice and assistance in the development of the Computer Security Training Guidelines.

3. Management Education - We will continue our management education effort by providing briefings on the Computer Security Act for Federal Executive Boards and Federal Executive Associations throughout the country. These briefings will be provided during the first and second quarters of FY 1989.

4. Hand-off Training Materials - We will distribute to

agencies in November, 1988, Computer Security Awareness training materials which we are preparing.

5. Interagency Training and Technical Assistance - We will expand our OPM interagency training offerings in Computer Security Awareness and in specialized subjects beginning in the first quarter, FY 1989, and continuing. We will also assist agencies, on request, to develop agency-specific Computer Security training materials beginning the first quarter, FY 1989, and continuing.

Computer Security Training Oversight - In order to carry out our oversight role, we need base-line data on what computer security training is now being provided by agencies and what training agencies will provide their employees on a continuing basis. Since the General Accounting Office has already begun a survey of Federal agencies which will collect the base-line data we need, we have concluded that it would be in the best interest of the government to use the GAO data, rather than conduct a duplicate survey. We have been told by GAO staff that their data will be available when it is released by the committee. At that time we will amalgamate the GAO survey data with data we will get from the Agency Computer Security Plans which are due to the National Institute of Standards and Technology and the National Security Agency not later than January 8, 1989. We anticipate having the data from these two sources amalgamated

by early Spring, 1989. At that time we will have a comprehensive view of current and planned computer security training in departments and agencies. Once we have base-line data, we will conduct compliance reviews using a variety of methods including questionnaires, agency site visits, and interagency workshops. We also plan to add a computer security training reporting requirement to our Annual Report on Government Training. This information will permit us to determine how well agencies are carrying out the requirement for a continuing computer security training program.

Oversight, which is our highest priority, is one of several parts of a comprehensive plan OPM has underway to help assure agencies meet the Computer Security Act training requirements. Our comprehensive plan also includes policy and guidance; development of generic computer security training materials for hand-off to agencies; education of senior Federal officials; Government-wide interagency computer security training available through OPM's training delivery network; and OPM assistance to agencies in the development of agency-specific computer security training materials.

Computer Security Policy and Guidance - Our interim Computer Security Training Regulation was our initial step toward providing direction and guidance to agencies. We will publish our final regulation in January, 1989. We also plan to re-examine the final regulation in the fourth quarter FY 1989, after we have more data on agency training, to

determine if further elaboration of the regulatory requirements is needed. Although NIST has lead responsibly for the development of the Computer Security Guidelines, we at OPM are working closely with the NIST staff to help complete the Guidelines. We are also helping NIST by coordinating comments on the Guidelines from Federal training officials. Since the Guidelines represent Government-wide guidance to all Federal agencies, we are using them as our authoritative source for the content of the Computer Security training materials which we are developing for agencies and for delivery through OPM's Interagency Training Program.

Hand-off of Training Materials - OPM has a major training materials development project underway which will assure that agencies have available generic training materials on computer security. These materials will be available to agencies in November, 1988 and will be produced in several formats to respond to different agency needs. We will make available a 20 minute video tape which highlights computer security awareness basics. A second product is a job aid which agencies can use to reach mass audiences who need to learn basic computer security responsibilities but do not require formal classroom training. A third product is a briefing package designed for agency managers, which provides an overview of computer security requirements from the management perspective and can be used in conjunction with the video tape. The fourth product is a one-day classroom package which includes all the instructor and student

materials needed to teach an intensive computer security course. This format is also designed to allow agency officials to include their agency's specific computer security requirements in the training session. The fifth product is a printed self-study training package which agencies can use to reach their employees at remote work-sites. Finally, we also plan to provide computer based instructional materials on computer security.

Management Education - OPM has taken the lead, in collaboration with NIST and OMB, to provide widespread management education on the training requirements in the Computer Security Act. Since passage of the Act, our three agencies have held two major workshops at the NIST facility for agency officials who have lead responsibility for implementing the Act. In addition, we have begun a series of briefings to reach top level Federal officials through the Federal Executive Boards and Associations located in all the centers of Federal population throughout the United States. We recently held our first FEB Briefing in New York City for over 100 FEB members and their key agency managers. We are also working directly with training director and computer security educators who play a key role in their agencies' computer security training.

Interagency Training and Technical Assistance - OPM is also expanding its interagency course offerings in both computer security awareness training and in the specialized courses

for agency computer personnel. In addition, we are including computer security awareness topics in appropriate seminars for managers and executives. Further, we have available a contractor resource which agencies can use to develop agency-specific computer security training materials.

Mr. GLICKMAN. Thank you.

Mr. MCCURDY. I think you have covered it very well. Mr. Lafferty, you have been sitting here for a long time this morning and it has been a long session. I don't get a lot of enthusiasm for the duties of OPM for this Act. I hope that you take back with you the concern that this Subcommittee has and I think it is unanimous that we expect to see this law implemented. We expect it to be done thoroughly and we would like to do it timely. This is an important issue. You all have an important role to play. If you don't play your role very well, then it is not going to be done as well as we would like for it to be done.

We would like to think that OPM strives for excellence and certainly we would like to see a little more enthusiastic support for these provisions. I hope you will take that message back with you to the Director. We would like to follow up. I can assure you that we will be watching this closely.

Thank you very much, appreciate your being here.

Our next witness is Mr. Francis McDonough, Deputy Commissioner, Federal Information Resources Management at GSA. Mr. McDonough, we appreciate your coming by here today. Your entire statement will appear in the record.

STATEMENT OF FRANCIS A. McDONOUGH, DEPUTY COMMISSIONER, FEDERAL INFORMATION RESOURCES MANAGEMENT, GENERAL SERVICES ADMINISTRATION

Mr. MCDONOUGH. Thank you.

Mr. Chairman, GSA has a modest role in the implementation of the Security Act but we have a lot of activity going on in the Government in the information resources management area. We have a good legislative base. We will be doing four things to help implement the Act.

First, we will help implement it into our Federal Information Resources Management Regulation. Secondly, we will be helping OMB develop the plan. Third, we will provide assistance to agencies on a contract schedule basis so they can acquire services easily, do the things they may need to do under the Computer Security Act. Fourth, there is a system of accountability. We do have two review programs where we review what agencies do with the authority we have given them and we review other aspects of their management program in the information resources management area.

In summary, those are the four things we will be doing to protect the data of the American people that they entrust to their computer systems.

[The prepared statement of Mr. McDonough follows:]

STATEMENT OF FRANCIS A. McDONOUGH
DEPUTY COMMISSIONER
OFFICE OF FEDERAL INFORMATION RESOURCES MANAGEMENT, GSA

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

SEPTEMBER 22, 1988

Good morning Mr. Chairman and members of the subcommittee. The General Services Administration (GSA) appreciates the opportunity to testify on this important issue. The Computer Security Act of 1987 is timely and very much needed to provide direction for the Federal government.

In our governmentwide role, GSA provides leadership across the government in Federal Information Resources Management in several ways. Regulations, implementing Congressional legislation, are provided through the Federal Information Resources Management Regulation (FIRMR) system. Second, we provide an extensive series of guidelines, bulletins, handbooks, and self inspection reference documents to all agencies to help them to implement the regulations and legislation. Finally, assistance is provided to agencies. This takes the form of direct, person-to-person assistance through our Agency Liaison Officer program; and, assistance is provided through a series of optional-use contract schedules programs through which specialized skills and services are made available to Federal agencies at reduced prices and in a timely manner.

While GSA's role in the Computer Security Act of 1987 is modest, we will be helping to implement the legislation through our regulatory system, by assisting the Office of Management and Budget in the planning process, and by providing specialized assistance to agencies. Let me address first how GSA will use its FIRMR regulatory system to implement the provisions of the legislation.

GSA will play an important and essential role in implementing within the Federal Government the computer security standards developed by the National Institute of Standards and Technology (NIST). The Federal Information Resources Management Regulations (FIRMR) system requires Federal agencies to use NIST standards in the management and use of information technology resources. In addition, the FIRMR requires Federal contracting officers to include NIST standards in solicitations for information technology resources. These key FIRMR policies will apply to computer security standards when the standards are published by NIST.

As individual computer security standards are published, GSA will work with NIST and Federal agencies, and the information technology industry to develop contract clauses for contracting officers to use in specifying the standards in Federal contracts.

3.

In addition, GSA will continue to update and publish the "ADP and Telecommunications Standards Index" which provides Federal agencies with a complete reference document on current NIST standards and related contract clauses to use in their contracting activities. As computer security standards are published by NIST, GSA will update the "ADP and Telecommunications Standards Index" to ensure agencies have a complete and up-to-date reference document.

GSA will continue to address agency use of NIST standards, including the use of computer security standards, during our reviews of individual agency information resources management activities. GSA conducts these management reviews to ensure that agencies follow Federal policies and procedures, and to determine the level of procurement authority to delegate to individual agencies.

The legislation establishes a requirement for agencies to develop individual security plans for systems containing sensitive information and to incorporate summaries of these plans in the agency's five-year information systems plan. GSA will assist the Office of Management and Budget (OMB) in developing governmentwide policies for this process and we will continue to assist OMB in developing the annual, five-year plan for the government.

4.

With regard to GSA plans to provide assistance to agencies it is important to point out that we have a history of providing assistance to agencies in addressing Security issues. For example, a contract for security risk analysis was first awarded on September 18, 1984. Eighty nine task orders for risk analysis services have been placed to date against this contract by Federal agencies. This contract covers the eastern and central portions of the United States and will expire on January 18, 1989.

Because of increased Federal interest in information security created by Public Law 100-235 and GSA's desire to ensure consistent implementation of the security services provided, GSA management determined that the best approach for the continued provision of these much needed security services is to award a single contract with nationwide coverage. Such a contract will be in place later this year.

Under this nationwide contract the contractor will make available a number of security services, including (1) Risk Analysis, (2) Contingency and Disaster Recovery Plans, (3) Security Test and Evaluation Plans, (4) Physical Security Audits, (5) Sensitive and Criticality Assessments, and (6) Security Training Awareness

Courses. These services will be available to Federal agencies on a voluntary basis by entering into interagency agreements with GSA. The contract, however, is not intended to be all encompassing or the only avenue of support to Federal agencies needing assistance in the security area. It is intended to supplement rather than supplant agencies' independent efforts to acquire such services.

GSA will ensure the quality of services rendered under this contract. Our goal is to provide uniform and consistent assistance to agencies in implementing the security requirements mandated by Federal law and regulation. In order that Federal agencies may remain abreast of the latest development in the security arena, the contractor will maintain an electronic bulletin board that client agencies will be able to access for the latest security advisories and guidance.

To complement the services that will be available under the nationwide security services contract, we are preparing a publication, "Information Technology Installation Security", to assist managers in defining and implementing physical security programs at Government facilities which handle sensitive information.

This publication defines the components of a security program and provides procedures for developing, implementing, and maintaining a practical and effective physical security program that:

Complies with laws, policies, regulation, standards, and guidelines influencing or directing security policy; and

Provides reasonable assurance that assets are protected from potential risks and threats.

During the next several months, GSA central and zonal offices and its contractor will conduct an awareness program designed to inform Federal agencies of the services available through GSA.

All of GSA's activities in providing assistance to agencies will be conducted in accordance with the guidelines and standards issued by NIST.

Mr. Chairman, I would like to thank you for the opportunity to discuss the actions GSA will be taking to help implement the Computer Security Act of 1987. We are serious about our responsibilities to help protect the data which the American people entrust to the computer systems of the Federal government.

Mr. GLICKMAN. I had previously written to you. I have written to the GSA about making sure that you give appropriate concern to 8-A firms and the relationship between this and the competitive selection processes.

What kind of competitive acquisition method is GSA using to provide for a follow on nationwide security services contract mentioned in your statement and is this an 8-A procurement?

Mr. MCDONOUGH. This will be an 8-A procurement, Mr. Glickman. We looked at the requirements and surveyed the 8-A community. We did identify a vendor who has a lot of experience in helping agencies like IRS and the Navy in these kinds of areas. We are going to proceed to contract.

Mr. GLICKMAN. Mr. McCurdy?

Mr. MCCURDY. I have no questions for you. Thank you very much.

Mr. GLICKMAN. Finally we have Mr. Howard G. Rhile, Jr., Associate Director, Information Management and Technology Division, General Accounting Office. We appreciate your coming by. We appreciate the report that you have provided to Chairman Brooks and Chairman Roe, which we have a copy of dated today. You may begin.

STATEMENT OF HOWARD G. RHILE, JR., ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE

Mr. RHILE. I, too, would like to briefly summarize my statement and request it be placed in the record.

Mr. GLICKMAN. It will be placed into the record.

Mr. RHILE. First of all, we do appreciate the opportunity to appear today and respond to your request for testimony on Federal agencies' progress in implementing this Act.

As you know, we are conducting a three part effort to determine whether Federal agencies are complying with specific requirements of the Act and meeting the deadlines of the Act.

My statement today summarizes the results of the first part of the work, which is for agencies to identify their sensitive systems. As mentioned, we did issue a report today which presents the details of that work.

With your permission, I'd like to place that report as well in the record.

Mr. GLICKMAN. The report will be included in the record.

[The information referred to follows:]

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-231257

September 22, 1988

The Honorable Jack Brooks
Chairman, Committee on
Government Operations
House of Representatives

The Honorable Robert A. Roe
Chairman, Committee on Science,
Space, and Technology
House of Representatives

In your February 23, 1988, letter you requested that we determine whether federal agencies are complying with provisions of the Computer Security Act of 1987. As agreed with your offices, we are conducting a three-part effort using questionnaires to determine federal agencies' compliance with specific requirements and milestones of the act. This report provides the status of federal agencies' compliance with actions required as of the first milestone, July 8, 1988. To obtain the status, we sent a questionnaire to 89 federal agencies not specifically exempted from compliance with the act. As discussed with your offices, we did not independently verify the agencies' responses to this questionnaire. A discussion of our objectives, scope, and methodology is contained in appendix I.

The Computer Security Act of 1987, PL 100-235, was enacted on January 8, 1988. The act provides for improving the security and privacy of sensitive information in federal computer systems. Section 5(c) of the act requires the Office of Personnel Management to issue training regulations prescribing the procedures, scope, and manner of security training to be provided to federal civilian employees. Section 6(a) requires federal agencies to identify computer systems under their supervision that contain sensitive information. These requirements were to be accomplished by July 8, 1988.

On September 16, 1988, we briefed your offices on the status of federal agencies' compliance with sections 5(c) and 6(a) of the act. This report summarizes the information discussed during that meeting.

Five of the 89 agencies to which we sent our questionnaire stated that they were not subject to the act. We agreed that three of them are not federal agencies as defined by the act, and are therefore exempt. A fourth stated that it was exempt because it did not have any federal computer systems as defined by the act. The fifth, the Central Intelligence Agency, said that it would send us documentation to support its reasoning that it was exempt from the act. As of September 16, 1988, we had not received this documentation.

It appears that federal agencies are attempting to comply with the act. Concerning the requirements of section 5(c), the Office of Personnel Management issued an interim training regulation on July 13, 1988, 5 days after the act's deadline. About 77 percent (65 of 84) of the federal agencies subject to the act reported to us that, as of July 8, 1988, they had identified all of their computer systems with sensitive information in compliance with section 6(a) of the act. An additional nine federal agencies reported that they had identified all of their computer systems with sensitive information as of September 8, 1988. Six federal agencies reported that they had not identified all of their sensitive systems as of September 8, 1988. They estimated that they would complete the identification by December 1988. Four federal agencies did not respond to our questionnaire. Three of these agencies initially told us they were uncertain as to whether they were subject to the act, but recently determined that they are subject to the act. They said they are in the process of identifying their sensitive systems. The National Security Council told us that it had not (1) decided whether to respond to our questionnaire or (2) identified its computer systems with sensitive information.

Should you have any questions about this report, please call me on 275-4892 or Howard Rhile, Associate Director, Information Management and Technology Division, on 275-9675.

Sincerely yours,

Ralph V. Carlone

Ralph V. Carlone
Director

Mr. RHILE. With regard to the training regulation that was due, OPM did indeed issue it on July 13th in the Federal Register and it became effective then.

It outlines Federal agencies' training responsibilities and points out that training should do three things. One, stress the vulnerability of computer systems; and two, be organized around the agency's security policies, practices and procedures; three and very important, be a continuous process.

With respect to determining Federal agencies' compliance with the Act's requirement to identify their sensitive systems, we sent a questionnaire to 89 Federal agencies that were not specifically exempted from the Act. Five of these agencies reported that they were not subject to the Act. After reviewing their reasoning, we agreed that three of them indeed did not fall under the Act. A fourth reported that it was exempted because it didn't have any Federal computer systems, as defined by the Act. The fifth agency, CIA, said it would send us some documentation to support its reasoning that it was exempt from the Act. We are awaiting that documentation.

If I may, I would now like to direct your attention to this chart before you. This chart represents the responses to the questionnaires that we sent to the 84 agencies that remained. I must point out that as discussed with your office, we did not independently verify the information that they sent us.

As of September 8th of this year, in response to our questionnaire, 74 agencies or about 88 percent responded that they had identified all of their sensitive systems. Six agencies as of that date reported they had not yet identified all of their sensitive systems but they estimated they would complete the identification by December and I think four of them said they would have it done in October. One of these six, the Department of Interior, told us a few days ago that it had completed the identification.

Four agencies did not respond to our questionnaire.

Mr. GLICKMAN. Which ones were those?

Mr. RHILE. They were the National Security Council and three legislative agencies. [Laughter.]

Mr. GLICKMAN. Which three legislative agencies?

Mr. RHILE. The Congressional Budget Office; Library of Congress and the Office of Technology Assessment. We contacted these agencies and they initially told us that they were unsure as to whether they were subject to the Act but they called us a few days ago and have determined they are indeed subject to the Act and they are taking action to comply.

Mr. MCCURDY. We will have Jack Brooks get on them. [Laughter.]

Mr. RHILE. If I may, I would like now to direct your attention to the second chart. This chart shows the numbers of sensitive systems that were identified by the agencies in response to our questionnaire. As shown on the chart, the Navy reported 27,000 systems or about one-half of the total systems reported. The Army reported 12,000 systems, about 23 percent; the Air Force reported 10,000 or about 19 percent; other DOD components, about 3,000; and the civilian agencies reported about 1,400 systems.

In summary, it appears that Federal agencies are attempting to comply with the requirements of the Computer Security Act. OPM's regulation became effective five days after the July 8th deadline. Based on our questionnaire responses, about 90 percent of the agencies as of today have identified their sensitive systems.

This concludes my summary.

[The prepared statement of Mr. Rhile follows:]

United States General Accounting Office

GAO Testimony

For Release
on Delivery
Expected at
9:30 a.m. EST
Thursday
September 22,
1988

STATUS OF COMPLIANCE WITH THE COMPUTER SECURITY ACT OF 1987

STATEMENT OF
HOWARD G. RHILE, ASSOCIATE DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
COMMITTEE ON SPACE, SCIENCE AND TECHNOLOGY

GAO/IMTEC-T-38-8

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to respond to your request for testimony on federal agencies' progress in implementing the Computer Security Act of 1987. As you know, at the request of two Chairmen, we are conducting a three-part effort to determine whether federal agencies are complying with specific requirements and deadlines of the act. My statement today summarizes the results of the first part of our work, federal agencies' compliance with the Act's July 8, 1988 requirements to issue training regulations and identify their computer systems that contain sensitive information. We are also issuing a report today that details the results of this work. With your permission, I would like to place it in the record of this hearing.

Our future work will focus on agencies' compliance with the Act's requirements to establish training programs and security plans for their sensitive systems.

Training Regulation Due By July 8, 1988

With regard to the training regulation due by July 8, 1988, the Office of Personnel Management distributed an interim regulation on this date entitled Training Requirement for the Computer Security Act at a government-sponsored briefing and seminar on implementation of the act. The interim training regulation became effective and was published in the Federal

Register on July 13, 1988. It outlines federal agencies' training responsibilities under the Act, and points out that training should

-- stress the vulnerability of computer systems;
-- be organized around the agency's security policies, practices, and procedures; and
-- be a continuous process.

On July 8, 1988, The National Institute of Standards Technology, formerly the National Bureau of Standards, also issued a training document entitled, Computer Security Training Guidelines. The purpose of these guidelines is to help agencies in developing and selecting training in computer security awareness and accepted security practices. The guidelines were prepared in consultation with the Office of Personnel Management.

Sensitive Computer Systems to be Identified by July 8, 1988

To determine federal agencies' compliance with the Act's requirement to identify their sensitive systems by July 8, 1988, we sent a questionnaire to 89 agencies that were not specifically exempted. Five of these agencies reported that they were not subject to the Act. After reviewing their reasoning, we agree that 3 of them did not fall under the Act's definition of a federal agency. A fourth agency reported that it was exempt because it did not have any federal computer systems as defined by the Act.

The fifth agency, the CIA, said it would send us documentation to support its reasoning that it was exempt from the Act.

SEE CHART I

I would now like to direct your attention to the chart before you. The chart shows the responses to the questionnaires mailed to the remaining 84 federal agencies. I must point out that, as discussed with your office, we did not independently verify the information in the agencies' responses.

In response to our questionnaire as of September 8, 1988

-- 74 agencies or about 88 percent responded that they identified all of their sensitive systems. Of these:
   -- 65 agencies reported they had identified their sensitive systems as of July 8, 1988.
   -- 9 agencies reported they had identified their sensitive systems after July 8, 1988.
-- 6 agencies reported they had not yet identified all their sensitive systems. These agencies--Agriculture, Interior, VA, FEMA, ICC, and FCC[1]--estimated they would complete identification by December 1988. I would like to note that Interior told us a few days ago that they had identified all their sensitive systems.
-- 4 agencies did not respond to our questionnaire as of September 8, 1988--the National Security Council and 3 legislative agencies, the Congressional Budget Office, the

[1] Mr. Rhile's prepared statement should have read "and SEC" instead of FCC.

Library of Congress, and the Office of Technology Assessment. These legislative agencies initially told us that they were unsure as to whether they were subject to the Act. They called us a few days ago, however, and have determined that they are subject to the Act and are taking action to comply. The National Security Council recently told us that it had not yet decided whether to respond to our questionnaire.

Numbers of Sensitive Systems Identified by Federal Agencies

SEE CHART 2

I would now like to direct your attention to the other chart which I brought with me today. This chart shows the number of sensitive systems identified by federal agencies.

Seventy-two of the 74 agencies that had identified all their sensitive systems reported the number of sensitive systems they identified:

-- Navy reported 27,000 systems or about one-half of the systems reported;
-- Army reported 12,000 systems, about 23 percent;
-- Air Force reported 10,000 systems or about 19 percent;
-- Other DOD components reported 3,000 systems, 6 percent; and
-- All civilian agencies reported about 1,400 systems or 3 percent of the total.

In summary then, it appears that federal agencies are attempting to comply with the requirements of the Computer Security Act of 1987. The Office of Personnel Management's training regulation became effective on July 13, 1988, five days after the Act's July 8, 1988 deadline. Based on our questionnaire responses, about 77 percent of the federal agencies had identified their computer systems with sensitive information by the July 8, 1988 deadline. And about 90 percent of the agencies have identified all their sensitive computer systems, as of today.

This concludes my prepared statement, Mr. Chairman. I will be pleased to answer any questions that you or others may have at this time.

Identification of Sensitive Systems: 84 Agency Responses to GAO Questionnaire as of 9-8-88

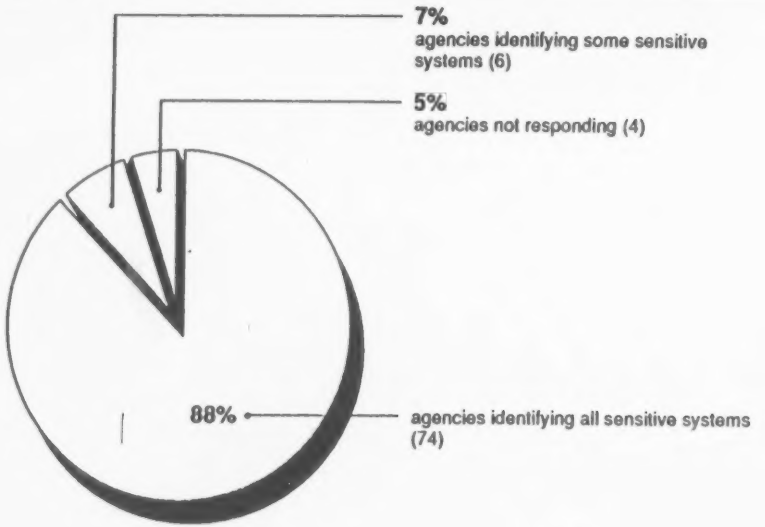

CHART I

Number of Sensitive Systems Reported by Agencies as of 9-8-88

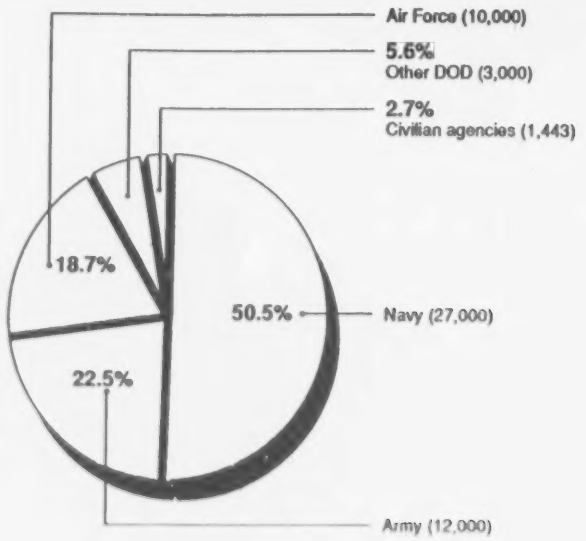

CHART 2

Mr. GLICKMAN. On these systems, are most of them operated by the agencies and how many of them are operated by contractors, private parties?

Mr. RHILE. We asked for that information in our questionnaire and of the agencies reporting as of September 8th, about 150 of them were identified as being operated by other than the agency itself. However, in looking at the DOD figures, we noticed they did not report any systems operated by contractors. We called them up and asked them about that. They told us they do indeed have those systems identified but they were unable at that time to break it out and they included the total in the total number they gave us.

Mr. GLICKMAN. You indicated that the CIA was one of the four agencies that did not respond. Are they claiming they are not covered under the Act?

Mr. RHILE. They are saying they don't believe they are and they are going to send us some documentation, as they characterized it, to support that reasoning. When we get that, we will evaluate it.

Mr. GLICKMAN. Will you share that material with us as well?

Mr. RHILE. We will be pleased to.

Mr. GLICKMAN. On balance, you believe that the Federal bureaucracy is complying with the law?

Mr. RHILE. I believe they are trying very hard to do so. The results that we got from our questionnaire plus our conversations with about 42 agencies indicates that.

Mr. GLICKMAN. Thank you. Mr. McCurdy?

Mr. MCCURDY. Did they cite any particular problems they were having?

Mr. RHILE. In complying? We asked them as part of our questionnaire for comments, comments on our questionnaire primarily, and the comments we got were some of the agencies were having difficulty gathering, putting together, the information that we had requested. Some of the agencies were having trouble getting the information from their components, the large agencies, such as Agriculture.

Mr. MCCURDY. I just share Mr. Glickman's view that we would like to see the justification from the CIA.

Mr. RHILE. We will be pleased to share that with you.

Mr. GLICKMAN. You are going to mail out a couple more questionnaires? You have a second questionnaire regarding training?

Mr. RHILE. That's correct.

Mr. GLICKMAN. Then you have a third questionnaire providing for security plans for sensitive information systems?

Mr. RHILE. That's correct.

Mr. GLICKMAN. What is your schedule for phases two and three of your audit?

Mr. RHILE. We are planning to send out the training questionnaire next week. We will be briefing the Committee on that in November. We expect to issue a report late December on that. On the security plans, we are planning to send that out around January 6th and issue a report on the results of that in May.

Mr. GLICKMAN. We will probably have some follow-up hearings. I yield back to the Chairman.

Mr. RHILE. We have been working very closely with Mr. Taylor on that.

Mr. McCURDY [presiding]. Since I am a member of the Armed Services Committee, I am a little more curious about the DOD breakdown. Is there any other follow-up that you will do with DOD on how specific those numbers are? I am surprised that Navy would be that much larger than Air Force, for instance. The Army I can understand, but Air Force, being on the R&D Subcommittee and seeing a number of the classified programs, I am a little surprised by that.

Mr. RHILE. These would be the unclassified ones. We are still working with DOD to provide us with a precise figure. They have offered to provide us lists of these, which we will probably take them up on.

Mr. McCURDY. 47,000, which would kill you with paperwork.

Mr. RHILE. It would be a long list.

Mr. McCURDY. Once you get more details on that and you are able to analyze it in more detail, would you provide that for us?

Mr. RHILE. We would be pleased to.

Mr. McCURDY. We will keep the record open for that. We will also keep the record open for a statement by the Chairman of the Government Operations Committee, Mr. Brooks, and other witness follow-up or questions.

If there are no further questions, we appreciate the testimony today and appreciate your report and look forward to hearing from you in the future.

Mr. RHILE. Thank you very much.

Mr. McCURDY. That concludes the hearing for today and again we appreciate the witnesses' time and look forward to working with you. Thank you.

[Whereupon, at 12:12 p.m., the Subcommittee recessed, to reconvene at the call of the Chair.]

[Information to be furnished follows:]

GAO United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-231257

December 8, 1988

The Honorable Dave McCurdy
Chairman, Subcommittee on
Transportation, Aviation and
Materials
Committee on Science, Space,
and Technology
House of Representatives

Dear Mr. Chairman:

During our testimony at the September 22, 1988, hearings on the Computer Security Act of 1987, the Subcommittee asked that we (1) provide the documentation that was promised by the Central Intelligence Agency (CIA) to support its belief that it was not covered by the act and our analysis of the documentation and (2) provide follow-up information with regard to the accuracy of the number of sensitive systems estimated by the Department of Defense (DOD).

CIA's Computer Systems

In our testimony, we said the CIA had reported to us that it was not covered by the Computer Security Act of 1987. We also said the CIA was sending some documentation to support its claim. On October 3, 1988, we received a letter from the CIA documenting its reasoning.

In its letter (attached), the CIA stated that it had determined that none of its systems are subject to the reporting requirements of the act. The CIA said its determination was based on 44 U.S.C. 3502(2), which is a provision of the Paperwork Reduction Act. We spoke with a CIA legislative attorney to obtain clarification of the agency's letter. The attorney stated that all of the CIA's computer systems, including administrative systems such as payroll, contain at least some classified or intelligence information and therefore are not subject to the Computer Security Act of 1987. According to the attorney, the CIA's computer systems are protected by stricter security requirements than those in the act.

B-231257

The Computer Security Act of 1987 does not specifically exempt from its coverage either the CIA as an agency or its computer systems. Section 3 of the act, however, effectively excludes from its application those computer systems that are excluded from the definition of automatic data processing under the Paperwork Reduction Act, 44 U.S.C. 3502 (2). That definition specifically excludes data processing or telecommunications systems that are involved with intelligence activities or cryptologic activities related to national security. Consequently, such computer systems are not subject to the requirements of the Computer Security Act.

Further, the Computer Security Act applies only to the security of sensitive information, a term that does not include classified information. Therefore, systems that process classified information are also excluded from coverage under the act.

In summary, if the CIA is correct that all of its computer systems either relate to intelligence activities or process classified information, then the CIA's computer systems are not covered by the Computer Security Act. We have no independent knowledge, however, of the nature or composition of the CIA's computer systems.

DOD's Estimate of Its Sensitive Systems

In our September 22, 1988, testimony before the Subcommittee, we said that in response to our questionnaire, DOD reported that it was in compliance with the Computer Security Act of 1987 and estimated that it had 52,000 sensitive systems as defined by the act. This estimate was composed of estimates made by DOD's components on the basis of implementation of DOD Directive 5200.28, dated March 21, 1988. This directive (1) uses essentially the same definition of the term sensitive information as is contained in the act and (2) requires the preparation of security plans for systems containing sensitive, unclassified information. DOD said the total estimate as well as its components' estimates were dependent on the system definition used by the various unit-level personnel. Also, in response to our questionnaire, DOD stated that the detailed inventories of sensitive systems were maintained at the unit level.

After the September 22, 1988, hearing, in response to our request, a DOD official stated that DOD would try to obtain more precise information on the number of sensitive systems

B-231257

of its components. However, on November 9, 1988, this official stated that DOD did not want to spend the time and resources necessary to obtain a detailed inventory of sensitive systems from each unit, unless requested to do so by the Subcommittee.

- - -

Should you have any questions about this letter, please contact me at 275-4892 or Howard Rhile, Associate Director, at 275-9675.

Sincerely yours,

Daniel C. White

Ralph V. Carlone
Assistant Comptroller General

Attachment

Central Intelligence Agency

Washington, D.C. 20505

2 September 1988

Mr. Howard Rhile
Associate Director
Information Management
and Technology Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Rhile:

The Director has asked me to respond to your 18 July 1988 and 3 August 1988 letters requesting completion of a questionnaire intended to determine federal agencies' compliance with section 6(a) of the Computer Security Act of 1987, Public Law 100-235, 8 January 1988.

After a thorough review of the various computer systems at the Central Intelligence Agency, we have determined that none of our systems are subject to the reporting requirements of the Act. This decision was based on 44 U.S.C. §3502(2).

Sincerely,

John L. Helgerson
Director of Congressional Affairs